



18 October 2022

Ref: OIA-2020/21-0364

Dear [REDACTED]

**Official Information Act request relating to Five Country Ministerial meetings**

I refer to your request made under the Official Information Act 1982 (the Act), transferred to the Department of the Prime Minister and Cabinet (DPMC) on 10 February 2021. Your request was for:

- “...the following information concerning the Five Country Ministerial meetings.*
- 1. When did New Zealand first attend a Five Country Ministerial meeting?*
  - 2. What are the dates and locations of all Five Country Ministerial meetings New Zealand has attended?*
  - 3. Why did New Zealand begin attending these meetings (ie what prompted New Zealand to start attending)?*
  - 4. Who made the decision that New Zealand should attend? Please provide all briefings and cabinet documents relating to New Zealand commencing participation in these meetings, and for each meeting attended.*
  - 5. Were there predecessor meetings to the Five Country Ministerial meetings and, if so, what were they called, what is the list of dates of New Zealand attendance and what was the reason for the change?*
  - 6. Are the Five Country Ministerial meetings part of wider formal government-to-government arrangements? If so, please describe these arrangements.*
  - 7. For each Five Country Ministerial meeting New Zealand has attended, who was the minister who attended, how many officials accompanied the minister and, for each of those officials, which agency did they work for and what was their position?”*

On 23 April 2021 I responded to parts 1 – 3 and 5 – 7 of your request. I also provided a partial response to part 4, releasing as able material prepared for the 2018 Five Country Ministerial (FCM) meeting held in Australia from 28-29 August 2018. I advised you that I would respond again in relation to the remainder of the material relevant to this part of your request as soon as consultations had been completed and the information had been fully prepared for release. The release of each of these briefings involved extensive consultation with the various agencies that contributed to the briefings. The ability of all agencies to carry out these consultations was impacted by competing priorities, including the response to the COVID-19 pandemic. I am now in a position to respond to the remainder of part 4 of your request. I apologise again for the delay in finalising the response to this part your request.

Please find **enclosed** the following briefings of the remaining FCM meetings held, as set out in table below. Some parts of these documents have been withheld under the following sections of the Act:

- Section 6(a), as the making available of that information would be likely “to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand”;

- Section 6(b)(i), as the making available of that information would be likely “to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government”;
- Section 6(c), as the making available of that information would be likely “to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial”;
- Section 9(2)(a), as withholding the information is necessary “to protect the privacy of natural persons, including that of deceased natural persons”;
- Section 9(2)(ba)(i), as withholding the information is necessary to “protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied”;
- Section 9(2)(c), as withholding the information is necessary to “avoid prejudice to measures protecting the health or safety of members of the public”;
- Section 9(2)(f)(iv), as withholding the information is necessary to “maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials”;
- Section 9(2)(g)(i), as withholding the information is necessary to “maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any department or organisation in the course of their duty”; and
- Section 9(2)(j) as withholding the information is necessary to “enable a Minister of the Crown or any department or organisation holding the information to carry on, without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)”.

Where information has been withheld under section 9 of the Act, no public interest in releasing the withheld information has been identified that would be sufficient to override the reasons for withholding it.

While it remains necessary to withhold parts of this information for reasons relating to international relations and national security, as noted above, links to the communiqués, which outline the Ministerial FCM discussions, are available on DPMC’s website at the following address: <https://dpmc.govt.nz/our-programmes/national-security/five-country-ministerial>.

In addition, as marked in the documents released to you, there is some further information that is already publicly available:

- There is some information included in the briefing for the 2016 meeting that is available on the NZ Police website at: [www.police.govt.nz/about-us/publication/cabinet-paper-whole-government-action-plan-reduce-harms-caused-new-zealand](http://www.police.govt.nz/about-us/publication/cabinet-paper-whole-government-action-plan-reduce-harms-caused-new-zealand). To the extent your request is for this information, it is refused under section 18(d) of the Act on the basis “that the information requested is ... publicly available.”
- There was a draft statement included as part of the 2020 meeting briefing. The final statement (12 October 2020) “International statement - End-to-end encryption and public safety” is publicly available on the Beehive website at: [www.beehive.govt.nz/release/international-statement-end-end-encryption-and-public-safety](http://www.beehive.govt.nz/release/international-statement-end-end-encryption-and-public-safety). To the extent your request includes the final statement, it is refused under section 18 (d) of the Act [as per above]. To the extent it is for the original draft statement, this has been withheld under section 6(a) of the Act, as outlined above.

I have taken a small amount of information in these briefing packs to be out of scope of your request, for example, administrative timetables for bilateral meetings that occur adjacent to the FCM sessions, as marked in the briefing material. The briefing pack for the 2021 FCM meeting

has not been included as at the time your request was made, the pack did not exist. If you would like to make a subsequent request for the 2021 (or 2022) material, please advise.

Please find an outline of the enclosed material below.

Doc No	Date and Location of FCM Meeting	Sections some information withheld under
Document 1	21 – 22 July 2013 Monterey, California	6(a), 6(b)(i), 9(2)(a), 9(2)(f)(iv), and 9(2)(g)(i)
Document 2	5 – 6 February 2015 London, United Kingdom	6(a), 6(b)(i), 6(c), 9(2)(a), 9(2)(g)(i), and 18(d)
Document 3	16 – 17 February 2016 Washington DC, United States of America	6(a), 6(b)(i), 6(c), and 18(d)
Document 4	26 June 2017 Ottawa, Canada	6(a), 6(b)(i), 9(2)(a), and 9(2)(g)(i)
Document 5	29-30 July 2019 London, United Kingdom	6(a), 6(b)(i), 6(b)(ii), 6(c), 9(2)(c), 9(2)(f)(iv), 9(2)(g)(i), and 9(2)(j)
Document 6	18 June 2020 Wellington, New Zealand	6(a), 6(b)(i), 9(2)(a), 9(2)(ba)(i), 9(2)(f)(iv), 9(2)(g)(i), 9(2)(j), and 18(d)

There were some additional documents provided for the meetings that have been withheld in full under the following sections of the Act:

- Section 6(a), [as per above]
- Section 6(b) as the making available of that information would be likely “to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by-
  - (i) the Government of any other country or any agency of such a Government.
  - (ii) any international organisation.”

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

As noted in my previous response to you, this response, together with the response provided on 23 April 2021, will be published on DPMC’s website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely



Tony Lynch  
**Deputy Chief Executive**  
**National Security Group**

- Enc:
- Briefing for meeting 21 – 22 July 2013, Monterey, California
  - Briefing for meeting 5 – 6 February 2015, London, United Kingdom
  - Briefing for meeting 16 – 17 February 2016, Washington, DC, United States of America
  - Briefing for meeting 26 June 2017, Ottawa, Canada
  - Briefing for meeting 29-30 July 2019, London, United Kingdom
  - Briefing for meeting 18 June 2020, Wellington, New Zealand



# Ministerial

AUSTRALIA CANADA NEW ZEALAND UNITED KINGDOM UNITED STATES

MONTEREY, CALIFORNIA

JULY 21- 22, 2013

NAME	CELLPHONE NO
Steve Brazier	s9(2)(a)
Warren Tucker	
Judith Collins	
Megan Wallace	
Carolyn Tremain	
Felicity Buchanan	
Aphra Green	





## FIVE COUNTRY MINISTERIAL DELEGATIONS

### AUSTRALIA

The Honorable Jason Clare, Minister for Justice, Minister for Home Affairs

s6(a)

### CANADA

The Honorable Stephen Blaney, Minister for Public Safety Canada

s6(a)

### NEW ZEALAND

The Honorable Judith Collins, Minister of Justice

Dr Warren Tucker, Director, New Zealand Security Intelligence Service

Ms Carolyn Tremain, Chief Executive and Comptroller of Customs

Mr Steve Brazier, Director, Security and Risk Group, The Department of the Prime Minister and Cabinet

Ms Megan Wallace, Senior Private Secretary to The Hon Judith Collins

Ms Felicity Buchanan, Divisional Manager, Ministry of Foreign Affairs and Trade

Ms Aphra Green, Policy Manager, Ministry of Justice

### UNITED KINGDOM

The Rt. Honorable Theresa May MP, Home Secretary

s6(a)

### UNITED STATES

The Honorable Janet Napolitano, Homeland Security Secretary

s6(a)

# MINISTERIAL DELEGATIONS

Australia (10)	Canada (7)	New Zealand (7)	United Kingdom (6)	United States (9)
The Hon. Jason Clare Minister for Justice Minister for Home Affairs	The Hon. Stephen Blaney Minister Public Safety Canada	The Hon. Judith Collins Minister of Justice	The Rt. Hon Theresa May MP Home Secretary	The Hon. Janet Napolitano Homeland Security Secretary
s6(a)	s6(a)	Dr Warren Tucker Director New Zealand Security Intelligence Service	s6(a)	s6(a)
		Ms Carolyn Tremain Chief Executive and Comptroller of Customs		
		Mr Steve Brazier Director Security and Risk Group The Department of the Prime Minister and Cabinet		
		Ms Megan Wallace Senior Private Secretary Hon Judith Collins		
		Ms Felicity Buchanan Divisional Manager Ministry of Foreign Affairs and Trade		
		Ms Aphra Green Policy Manager Ministry of Justice		

Released under the Official Information Act 1982

# DRAFT Agenda

Five Country Ministerial  
Monterey, California  
July 21 – 22, 2013

## Sunday, July 21

1200 1745 Bilateral Meetings  
1800 1900 Reception hosted by the Australian Delegation  
1930 2100 Ministers' only dinner (off-site)

---

## Monday, July 22

0900 0945 Intelligence Briefing  
s6(a)

1000 1030 Opening Remarks by each Minister  
Open press, no Q&A

1030 1130 **Session One:** The Cybersecurity of Critical Infrastructure  
s6(a), 6(b)(i)

1130 1145 Tea Break


1145 1245 **Session Two:** Countering Violent Extremism  
s6(a), 6(b)(i)

DRAFT as of: Thursday, July 18, 2013

1245 1345 Ministers' Lunch

1400 1500 **Session Three: Data Exchange Initiatives**


s6(a), 6(b)(i)



1500 1515 Tea break

1515 1615 **Session Four: Ministerial Strategic Direction**

s6(a), 6(b)(i)



1630 1700 Closing Remarks

1700 Meeting Adjourns





## INTELLIGENCE BRIEFING

Hon Judith Collins, Minister of Justice

### Talking points

- The brief has set the scene for discussions going forward and highlights issues of security reach across a variety of policy and operational portfolios. It is imperative that we bring these areas together to ensure we optimize our outcomes.
- However I note that New Zealand has a significantly different threat environment to most, if not all, of the partners represented here.

s6(a)

s6(a)

s9(2)(g)(i)

### Objectives/Key points

- Ministers are expected to receive a classified briefing at the commencement of the meeting which sets out the key elements of the violent extremism and terrorism threat environment.
- New Zealand's threat environment differs significantly to that of many of our partners, however we see limited reflections in New Zealand of the activities likely to be discussed.
- The information provided at this briefing will inform discussions in session two – countering violent extremism (CVE). That session contains recommendations for action and will be subject to a separate briefing note.

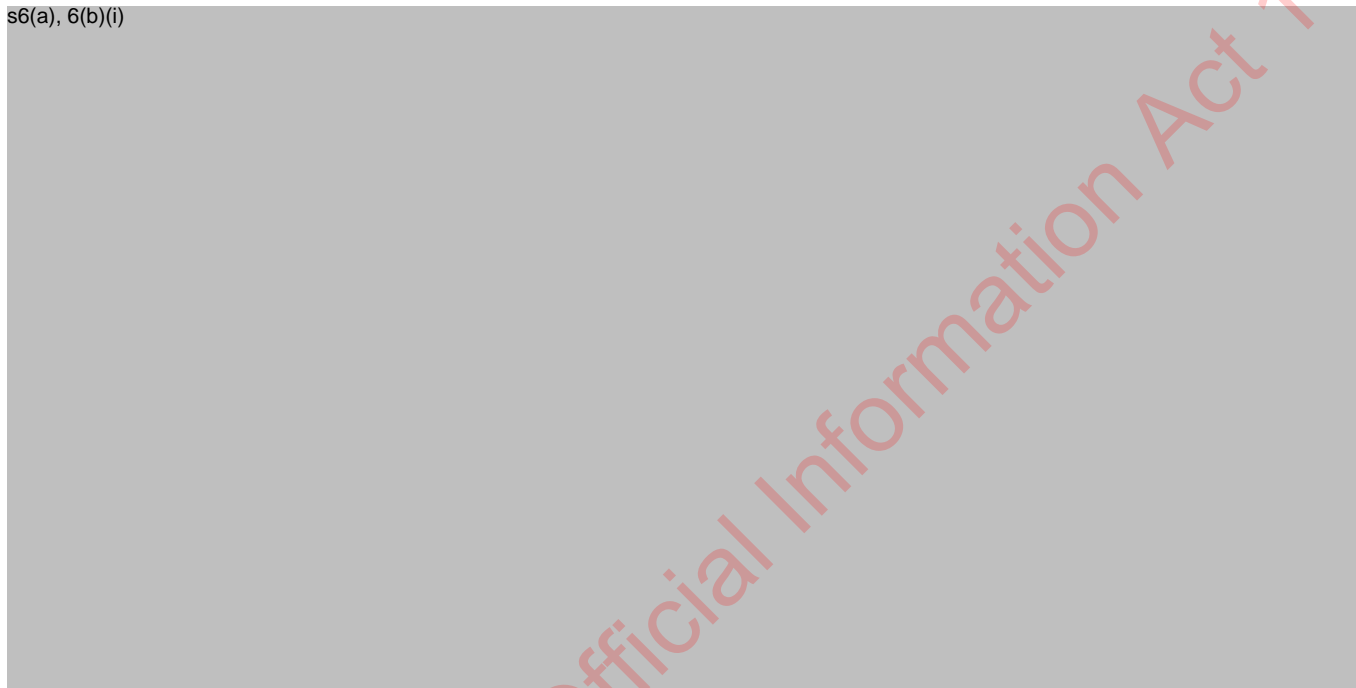
## Background

---

We anticipate from the papers provided that the meeting will commence with a classified briefing on the international threat environment. The main themes to be covered during this briefing are likely to be reflected further during elements of the meeting and include:

### *International trends:*

s6(a), 6(b)(i)



### *Domestic issues:*

- the relative success in terms of both publicity and harm that can be achieved by lone actors, often inspired but not directed by AQ (referred to as **Homegrown Violent Extremism**, examples include Boston, Woolwich) and the ongoing threat from non Islamic domestic terrorism (for instance White Supremacy movements).

### **New Zealand threat environment**

When we consider the New Zealand threat environment <sup>s6(a)</sup> [redacted], what becomes immediately apparent is that many of the issues faced by our partners are not similarly experienced in New Zealand. The current threat level for New Zealand has been set at VERY LOW.

s6(a)



Released under the Official Information Act 1982

Released under the Official Information Act 1982



Classified material has been printed on colored paper to assist in managing material across the classified and unclassified/restricted spaces.

Released under the Official Information Act 1982

**OPENING REMARKS**

Hon Judith Collins, Minister of Justice

I would like to thank Secretary Napolitano and her officials for organising and hosting this meeting. In preparing for this meeting I have been impressed by the range and depth of cooperation between our five countries. As Ministers, we have an opportunity to offer strategic oversight of these activities and to provide additional impetus where this might be required.

Data exchange, cyber-security and counter-terrorism are the key themes running through all of today's sessions. Increased global connectedness, through travel and the internet, means New Zealand can no longer rely on its geographical isolation for protection. s9(2)(g)(i)

New Zealand enjoys significant benefits from the exchange of data between our five countries such as visa-free travel entry into over 50 countries. It is clear that there are opportunities to facilitate greater data exchange and I am keen to explore these, recognising that we must also deal with privacy, policy and technical challenges. New Zealand and Australia have worked closely on improving data exchange in a number of areas and our experience may be able to inform five countries work.

I would like to emphasise the importance of publicly conveying the benefits that the five countries relationship, and data exchange, offer all of our citizens. In New Zealand, and in other countries too, there is natural concern about the sharing of information within and between government agencies and international partners by some interest groups, media and members of the public. Therefore there needs to be greater focus on communicating to the public about data exchanges – what they

**OPENING REMARKS**

**Hon Judith Collins, Minister of Justice**

are, and what they are not - so that the public better understand the value of these initiatives. Being able to successfully implement new data exchange programmes will, to a large extent, depend on our governments having the support and trust of the public.

I look forward to today's discussions. I am optimistic that they will lead to concrete actions and that we can build on our already collaborative relationship.

And in closing I would like to take this opportunity to wish Secretary Napolitano all the best in her new role as President of the University of California –a role that will no doubt bring just as many – but very different – challenges to those she has faced in her political career.

## SESSION ONE: THE CYBER SECURITY OF CRITICAL INFRASTRUCTURE

Hon Judith Collins, Minister of Justice

### Introduction

- s6(a) is leading Session One. The main agenda paper is 'Cybersecurity of critical infrastructure'. The session will discuss ways in which the countries could cooperate to protect critical infrastructure from cyber threats (such as espionage and sabotage).

- s6(a), 6(b)(i)

### Talking points

#### Paper on the cyber security of critical infrastructure

- In New Zealand we're acutely aware that our critical infrastructure is vulnerable to cyber threats. In the past New Zealand relied on time and distance – the vastness of the South Pacific Ocean – to shield us against enemies.
- But now there's a new game. The advent of the Internet, and the way it globally connects people and machines almost instantly, means that time and distance are no longer barriers. We are just as vulnerable as everyone else, and that includes our critical infrastructure.
- The New Zealand Government is very serious about protecting our critical infrastructure from cyber threats. Among other initiatives, we've set up the National Cyber Security Centre, the NCSC, within the Government Communications Security Bureau. The Centre is working closely with counterpart agencies in the other Five Eyes nations, s6(a).

- s6(a)

- So, I see real value in the proposals that are set out in this paper. It makes good sense for us to be better coordinated, and to share our collective expertise. New Zealand can learn a lot from other Five Eyes nations, and in return we can offer our expertise and knowledge in this field.

s6(a), 6(b)(i)

s9(2)(g)(i)



Released under the Official Information Act 1982

Released under the Official Information Act 1982

#### *Definition of critical infrastructure*

- The New Zealand Government defines critical infrastructure as that needed to provide critical services, whose interruption would have a serious adverse effect on New Zealand as a whole, or on a large proportion of the population, and which would require immediate reinstatement.
- The Government's current focus is on six broad sector groups: communications (including the Internet); finance and economy; utilities; transportation; emergency services and major hospitals; and Government.

#### *New Zealand Government initiatives*

- The NCSC and the Department of the Prime Minister and Cabinet (DPMC) are working together, and with other agencies, on a range of initiatives to enhance the protection of critical infrastructure. These include:

s6(a)



## ***Paper on access to data***

### *The New Zealand Government's approach to data retention*

- s9(2)(f)(iv)
- 
- 
- 
- The Ministry of Justice is also leading work to consider New Zealand's accession to the Council of Europe Convention on Cybercrime, which will require a specific data preservation order regime.



SESSION TWO: COUNTERING VIOLENT EXTREMISM

Hon Judith Collins, Minister of Justice

Talking points

- As I previously advised, New Zealand's counter terrorism environment is different to those of the other countries attending talks.

s6(a)

I note:

- New Zealand is aware of limited cases of its citizens acting as *foreign fighters*.
- *Broken travel* (a process by which the end destination is concealed by itinerary splitting or passport changing) is very difficult to detect and easy to use from New Zealand due to the lack of direct flights to destinations of interest. Broken travel is not an indicator of radicalisation, but can be an attempt to hide the final destination for a number of other reasons (including criminality).

s6(a)

- The ability for individuals to access *information via the internet* in support of extremist activity remains of concern. New Zealand is not immune to this trend, however we have seen little evidence to indicate accessing material of this nature has translated into action. New Zealand agencies have not seen New Zealanders produce material of concern while onshore.

- A number of the recommendations put forward in the paper are outside New Zealand's immediate scope for delivery for a variety of reasons or replicate work already being done in the classified space.

s9(2)(g)(i)

s6(a)

s9(2)(g)(i)

Released under the Official Information Act 1982

6(a)



## Background

---

### CVE in New Zealand

- The lead agency for CVE programmes in New Zealand is the New Zealand Police. 6(a), 6(b)(i)



6(a)




### AGENDA ITEM 3 – Data Exchange Initiatives

Hon Judith Collins, Minister of Justice

#### Talking points

---


s6(a), 6(b)(i)



#### General comments

- I can see that exchanging more data between the Five Countries could have significant potential benefits for the public safety of our countries and for successfully identifying and managing high risk movements across our borders.
- I consider that future developments in sharing information between our countries should be undertaken where it can clearly be justified, where it can satisfy privacy concerns and where it does not unduly impinge on trade and travel facilitation objectives.
- I note that the Five Country working groups are all considering ways to enhance information sharing to improve security and suggest that enhancing the coordination between them may assist with this.
- New Zealand's experience of information sharing is that practical difficulties, like timeliness and the demand for real time sharing, can impede sharing intentions and need to be addressed.

s6(a), 6(b)(i)



### Objectives

- New Zealand can **support** the recommendations in the paper '**in principle**'. The recommendations refer to a large programme of potential initiatives that involve complex issues. In some cases, these issues will require significant effort to resolve.

- s6(a)

Released under the Official Information Act 1982



## Background

---

### *General comments*

- The Data Exchange Initiatives paper has been developed by s6(a) officials. New Zealand officials have had considerable input.
- The need for greater data exchange is arising, in part, from the increasing volumes of travellers and trade and the expectations about ease of movement across borders. Authorities need to work with international partners to address emerging cross-border threats. Examples are: human trafficking, illegal migration and organised crime including identity fraud and money laundering.
- Citizens expect their government to increase the benefits of trade, tourism and immigration while also protecting our countries from the associated risks. This pressure is occurring at a time when, due to the global financial crisis, the ability of governments to apply additional resources to border security is constrained.
- The Five Countries can work together to address these issues by leveraging collective capabilities, data, and resources to enhance the service, security, and efficiency of immigration and border systems.
- Already, the Five Countries are regularly sharing some information and intelligence through bilateral and multilateral arrangements. Existing policy and legislation in the Five Countries limit what can be shared, with whom, and there are identified impediments to sharing information due to technological and procedural weaknesses.
- These limitations need to be addressed by the Five Countries to enable greater information sharing. The Five Country working groups are currently cooperating to overcome these limitations; however, the issues are complex and dedicated resources are required to resolve the problems at hand.

s6(a), 6(b)(i)

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

*Current New Zealand Police arrangements to combat serious & organised crime*

- New Zealand Police has entered into a number of arrangements with the Strategic Alliance Group (SAG) partners to combat serious and organised crime, drug trafficking, targeting high risk offenders and collaborating on areas of mutual interest.
- There are formal arrangements with all SAG partners except Canada. The following arrangements involve information sharing for law enforcement purposes, within the constraints of relevant privacy laws within both countries:

s6(a)

**New Zealand-based initiatives that contribute to this topic**

*New Zealand Customs' Integrated Targeting and Operations Centre*

- The New Zealand Customs' Integrated Targeting and Operations Centre (ITOC) is a multi-agency border sector fusion centre. Aside from NZ Customs, Immigration NZ and Ministry of Primary Industries have seconded staff and New Zealand Police, Maritime New Zealand and NZSIS staff are also present.
- The ITOC is the best mechanism for bringing together border-related data sharing practice for operational use. The ITOC mission is to support the command and coordination of border sector operations, across New Zealand. All of the data required to determine the risk presented by specific goods, people or craft anywhere in New Zealand is brought together at the ITOC and operations are initiated, planned and coordinated from there.
- The ITOC is connected to targeting centres (NTC) in the other four countries:
  - Australia Customs and Border Protection Service's Passenger Analysis Unit
  - US targeting centres for passengers and cargo<sup>1</sup> and the International Targeting Centre<sup>2</sup>
  - the Canadian NTC, but communications are mostly filtered through the Liaison Officer in Canberra
  - the ITOC is working on securing direct communications with the United Kingdom's four NTCs.

*Future information sharing capability - Joint Border Management System*

- New Zealand Customs and the MPI are developing a fundamental change to border management by introducing the JBMS. The JBMS will enable cross-agency collaboration and coordination and allow for better use of resources through operating a joined up system. It will:
  - deliver a modern, integrated information system
  - ensure a coordinated approach for the delivery of public services to industry and the public

<sup>1</sup> The National Targeting Center – Passengers (NTC-P) and the National Targeting Center – Cargo (NTC-C).

<sup>2</sup> s6(a), s6(b)(i)



- enable the advance electronic submission of craft and cargo import and export clearance data, once, through a single entry point (Trade Single Window)
- enable facilitation of legitimate trade and travel.

*Future information sharing capability - Maritime Domain Awareness*

- New Zealand has a National Maritime Coordination Centre (NMCC). The NMCC is responsible for the overall management and control of New Zealand's maritime surveillance. Its role is to coordinate maritime patrol and surveillance activities in support of New Zealand agencies responsible for: maritime sovereignty and security; marine resources; law enforcement (including customs and immigration infringements); maritime safety; and environmental protection.
- The NMCC is in regular communication with the NZ Customs ITOC and engages closely with international partners in the region. Member agencies to the NMCC are New Zealand Defence Force; New Zealand Customs Service; Ministry of Fisheries; Department of Conservation; Ministry of Foreign Affairs and Trade; Maritime New Zealand; and the New Zealand Police.
- NZ Customs is scoping work to further develop New Zealand's maritime domain awareness and response to risks in the maritime environment from the movement of goods, people and craft.
- There is scope for greater collaboration with the Australia Customs and Border Protection Service (ACBPS) to manage maritime risk, including exchange of electronic data. ACBPS is currently seeking a secure data link with New Zealand to share craft reporting and risk information with their Border Enforcement Operations System (BEOS).

Released under the Official Information Act 1982

Released under the Official Information Act 1982

# FIVE COUNTRY MINISTERIAL



National Security / London 2015

## Thursday 5 February

Arrival from 15:00

Bilateral meetings

Out of scope

18:00-20:00

**Reception**

19:30-21:00

**Ministerial Dinner** - Intelligence Narrative (Ministers only)

## Friday 6 February

Arrival from 08:00

08:30-09:00

**Opening Remarks**

09:00-09:45

**Intelligence Briefing**

s6(a)

09:45-10:45

**Session One: CT - Countering Violent Extremism**

s6(a)

10:45-11:00

Tea Break

11:00-12:15

**Session One (continued): CT— Terrorist Travellers /  
Information sharing**

s6(a)

**OFFICIAL -- SENSITIVE**

12:15-13:15	<b>Lunch</b> (Minister plus 3) <b>Discussion on 5Eyes fora</b>
13:15-14:05	<b>Session Two: Cyber Security</b> s6(a)
14:05-14:55	<b>Session Three: Foreign Investment in Critical Infrastructure</b> s6(a)
14:55-15:15	Tea Break and Family Photo
15:15-16:05	<b>Session Four: Serious &amp; Transnational Organised Crime (CSE)</b> s6(a)
16:05-16:30	<b>Strategic vision / Communiqué</b>
16:30-17:00	<b>Closing Remarks</b>
17:00	Meeting adjourns

Released under the Official Information Act 1982





**New Zealand Intelligence Community**  
*Te Rōpū Pārongo Tārehu o Aotearoa*

## Briefing Note

26 January 2015

**To** Hon Christopher Finlayson: Minister in Charge of NZSIS; Minister Responsible for GCSB

**From** Howard Broad, DCE: Security & Intelligence, DPMC

**For your** Information

**Subject** **Five Countries Ministerial: Session One – Counter-Terrorism (Part 1 - Countering Violent Extremism)**

## Purpose

1. This note briefs you on the joint s6(a) topic for the counter-terrorism session of the upcoming Ministerial. It has primarily been prepared by the Department of the Prime Minister & Cabinet in consultation with the Department of Internal Affairs, Police and NZSIS.

## Background

2. s6(a), 6(b)(i)

## Foreign Fighters

3. Foreign fighters are a significant national security concern to each of our five country partners. s6(a), 6(b)(i)

4. The foreign fighters phenomenon is also an issue of increasing concern to New Zealand. As the Prime Minister has acknowledged publicly, New Zealand is not exempt from citizens travelling to fight in conflict zones. A small number of New Zealanders are known to have travelled to Syria s6(a). And the Minister of Internal Affairs has cancelled the passports of some New Zealand citizens who intended to travel to Syria.

### New Zealand's response to foreign fighters

5. Beyond the cancellation of passports, New Zealand's approach to foreign fighters seeks to address this issue in a broad-based manner, including working closely at the grass roots level with community leaders to build community resilience and maintain social cohesion.
6. New Zealand Police are currently considering ways to strengthen its approach to national security and violent extremism. While the risk in New Zealand continues to be low compared to our other five country partners, Police are working to ensure that their arrangements remain responsive to the changing threat environment.

#### 2014 legislative changes

7. In December 2014, amendments were made to the Customs and Excise Act 1996, the New Zealand Security Intelligence Service Act 1969 and the Passports Act 1992 following Parliament's consideration under urgency of the Countering Terrorist Fighters Legislation Bill. The changes enhanced agencies' powers to monitor and investigate, and to restrict and disrupt the travel of, foreign terrorist fighters. All three sets of changes came into force on 12 December 2014, and are subject to a sunset clause that expires on 1 April 2017. A summary table of the changes has been provided with this note.
8. The amendments were intended to help the NZSIS and other agencies manage the changed threat environment in New Zealand. s6(a)
9. The NZSIS also received a 15 percent increase to its funding over two years s6(a). s6(a); recruitment of new personnel is now underway.
10. These were a series of short-term measures to address the most immediate issues. The expectation is that any long-term changes required to NZ's legislative framework will be identified by the 2015 Review of the intelligence agencies, which is due to begin soon. Similarly, the long-term resourcing of the NZSIS and other agencies of the NZ intelligence community is under review and will be considered by Cabinet soon.

*Building resilient communities*

11. s6(a)
12. s6(a)
- New Zealand would regard many of the community based projects delivered under these "CVE Strategies" as worthwhile in and of themselves without being specifically tied to a CVE agenda. Community policing initiatives, or youth leadership programmes for immigrant communities, for example, deliver obvious public goods. They support social inclusion, strengthen community resilience to any potential radicalising influences and thereby reduce the risk of violent extremism as a secondary benefit.
13. s6(a)
14. In light of this, the New Zealand approach to the CVE question is focused as much, perhaps more, on ensuring that New Zealand's social harmony is protected as on legislative and law enforcement responses to terrorist threats. s6(a)
15. The Office of Ethnic Affairs has taken the lead on bringing together a cross-agency group of officials to discuss engagement strategies and initiatives to support New Zealand's Muslim communities. Officials from Police's MPES (Maori, Pacific and Ethnic Services), DPMC (Security & Intelligence Group), NZSIS, MFAT and Corrections have also participated. The two driving forces in this work are the Office of Ethnic Affairs and MPES – both of whom already have strong established relationships with community groups and leaders.
16. The intention of the joint group is to maximise efforts across government to enhance social cohesion and to work with communities to identify and address factors which could motivate individuals to engage in extremist activities. The Office of Ethnic Affairs is working on a paper for their Minister which is likely to outline the following three broad propositions:

- a. By tackling social problems such as poverty, unemployment, access to education, and poor housing, the Government is indirectly tackling the conditions that encourage youth to become disaffected and therefore vulnerable to anti-social influences.
- b. There is a need to build on current community engagement activities in order to reduce marginalisation and promote social cohesion, particularly as New Zealand's demographic profile continues to shift. A continuing focus on fostering positive relationships will be recommended over efforts to deliberately prevent destructive ones.
- c. The paper is also likely to recommend that engagement activities should not be linked directly with any agenda to "counter violent extremism."

17. s6(a)

#### *Dealing with those who have already been radicalised*

18. Strategies to tackle vulnerable individuals who have been radicalised are at present largely focused on the security intelligence and law enforcement options – ie the recent changes to legislation to better enable NZSIS to deal with persons of concern, etc. s6(a), 9(2)(g)(i)

19. Australia's recently developed National CVE Intervention Framework (CVEIF) is a whole-of-government initiative that aims to encourage and support the disengagement of young people from violent extremism. The CVEIF provides specific tools and overarching guidance for the support, referral and intervention processes which assist individuals to disengage from violent extremism. The objective of the framework is to connect individuals identified as at risk (through behavioural indicators) with services to assist with diversion and disengagement.
20. The CVEIF's tools and guidance will be made available to New Zealand as a full member of the Australia New Zealand Counter-Terrorism Committee (ANZCTC). Membership of this committee ensures the closest possible sharing of information between the two countries regarding all



aspects of counter-terrorism, and will be a good forum to focus New Zealand thoughts on progressing this aspect of CVE.

s9(2)(a)



Catriona Robinson  
*(for Howard Broad)*  
Director, National Security Systems  
Security & Intelligence Group  
The Department of the Prime Minister & Cabinet

30 January 2015

Released under the Official Information Act 1982



Comparison of Ministerial responsibilities – Homeland Security issues - Quintet countries

Responsibilities	s6(a), 6(b)(i)	NZ									
		PM	Minister for NZSIS GCSB	Minister of Justice	Minister of Police	Minister of Customs	Minister of Civil Defence and Emergency Management	Minister for Communications and Information Technology	Minister of Health	Treasury + (Ministry of Business, Innovation & Employment)	Minister of Immigration
Bankruptcy and financial crime policy/ fraud				✓ Financial Crime							
Border control (other than quarantine and immigration)					✓						
Border protection					✓						
Counter-terrorism capability development		✓	✓	to an extent	✓						
Communication Data/ Lawful Interception			✓					✓			
Crime Prevention				✓	✓						
Criminal justice				✓							
Critical infrastructure			✓ Cyber					✓		✓	
Cyber		✓						✓			
Emergency management/crisis coordination							✓				
Firearms					✓						
Illicit drugs				✓	✓	✓			✓		
International Crime Cooperation casework				✓	✓						
Law enforcement and policing				to an extent	✓						
National security law and policy		✓		to an extent							
Organised crime				✓	✓						
People smuggling						To an extent					✓
Proceeds of crime				✓							
Telecommunications surveillance law				✓				✓			



**New Zealand Intelligence Community**  
*Te Rōpū Pārongo Tārehu o Aotearoa*

## Briefing Note

28 January 2015

**To** Hon Christopher Finlayson, Minister Responsible for GCSB; Minister in Charge of NZSIS

**From** Howard Broad, DCE: Security & Intelligence, DPMC

**For your** Information

**Subject** **Five Countries Ministerial: Session Three – Foreign Investment in Critical Infrastructure**

## Purpose

1. This note briefs you on s6(a) the foreign investment in critical infrastructure session of the upcoming Ministerial. It has primarily been prepared by the Office of Overseas Investment (OIO) in consultation with Treasury and DPMC.

## Background

2. The Five Country Ministerial (FCM) was established in 2013; in part to improve overall ministerial oversight of the existing five country working groups and to ensure their work programmes are focussed on shared priorities. Established in 2012, the Critical Five is a five country working group focused on critical infrastructure protection. Noting the potential risks that can arise from foreign investment in critical infrastructure, the FCM will invite the Critical Five to include sharing best practice on managing foreign investment into critical infrastructure on its forward work programme. The aim of this work is to seek a balance between encouraging investment to support growth while maintaining security of infrastructure and infrastructure ownership. An overview of the Critical Five is contained at Appendix A.

s6(a), 6(b)(i)

4. The OIO gathers a significant amount of data about the investors who seek consent under the Overseas Investment Act 2005 (the Act). A significant amount of data is also gathered about the investment. After a consent or decline decision is made, information about the investor and the investment is released, in summary form, on the OIO's website. Normally these decision summaries are released at the end of the month following the date of the decision. As part of the decision summary release, statistical information is also made available each month about investments, primarily in aggregated form.
5. The OIO also has the ability to query its database answer specific queries in relation to the data held by it, for example, the production of country specific investment trends.
6. Some of the information held by the OIO about an investor may be information about an identifiable individual (personal information). Principle 11 of the Privacy Act states that an agency that holds personal information shall not disclose that information to a person or body or agency unless the agency believes on reasonable grounds that disclosure of the information is necessary, for example, to prevent or lessen a serious threat the public health or public safety, or that non-compliance is necessary (for example) to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, prosecution and punishment of offences, or (for example) that the information that will be disclosed is in a form that is non-identifying and used for statistical or research purposes.
7. Accordingly, while the OIO does have a significant amount of information, there are some limits on the information that can be made available (for example, the restrictions under the Privacy Act described above). In addition, the information held by the OIO only relates to the applications for consents that have been filed (and does not include investments that do not come within the applicable thresholds in the Act), or include investments that may have been entered into in breach of the Act (that the OIO does not know about).
8. These are some preliminary observations about some of the barriers to sharing investment information relevant to foreign investment in critical infrastructure, and more work will need to be done in this area, as the paper identifies.

### Managing foreign investment: the position in New Zealand

9. Free Trade Agreements entered into by New Zealand will typically contain a "security exception" clause, such as article 201 of the 2008 New Zealand China Free Trade Agreement<sup>1</sup>, which states:

<sup>1</sup> At page 115. There is an identical provision in Article 20.2 of the New Zealand Korea Free Trade Agreement (initialled by Chief Negotiators on 22 December 2014, but yet to be signed by Trade Ministers and ratified).

## Article 201 Security Exceptions

1. Nothing in this Agreement shall be construed:
  - (a) to require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests;
  - (b) to prevent a Party from taking any actions which it considers necessary for the protection of its essential security interests
    - (i) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials or relating to the supply of services as carried on, directly or indirectly, for the purpose of supplying or provisioning a military establishment;
    - (ii) taken in time of war or other emergency in international relations;
    - (iii) relating to fissionable and fusionable materials or the materials from which they are derived; or
  - (c) to prevent a Party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security ...

10. Article 202 1.(c) of the New Zealand China Free Trade Agreement states that where a party is in serious balance of payments and external financial difficulties or under threat thereof, it may, in the case of investments, adopt or maintain restrictions with regard to the transfer of funds related to investment, including those on capital account. However, the ability to exercise that power is subject to a range of restrictions aimed at ensuring the power is applied in a non-discriminatory and in the least restrictive way possible, and cannot be adopted or maintained for the purpose of protecting a particular sector.
11. The New Zealand Korea Free Trade Agreement also contains a provision Article 13.5 which states that nothing in Chapter 13 (Government Procurement) shall be construed to prevent any Party from taking any action or not disclosing any information which it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes.

### The Overseas Investment Act 2005 and free trade agreements

12. The principal obligations of free trade agreements in the area of investment relate to "national treatment" (NT) and "most favoured nation" (MFN) non-discrimination measures. Under the NT obligation, New Zealand is required to treat all established investments made by investors of the other party no less favourably than other investments. Because the obligation only applies post-establishment, the Act continues to apply to proposed investments in New Zealand by investors of the other party. The MFN obligation applies in respect of the treatment of all investments, both before and after establishment in the host market. This obligation requires that any better treatment relating to investment that New Zealand extends to third countries

must also be extended to the other party. Normally the MFN obligation only relates to future "better treatment" agreements, not agreements already entered into.

### The Overseas Investment Act 2005 and national security/critical infrastructure issues

13. The Act does not specifically deal with national security issues. However, all investors must meet criteria set out in the Act for consent under the Act to be granted. The criteria differ, depending on the investment type<sup>2</sup>. However, there are four criteria for consent ("the investor test") that are common to all investment types – that the relevant overseas person:

- has business experience and acumen relevant to the investment;
- has demonstrated financial commitment to the investment;
- is of good character; and
- is not an individual of a kind referred to in section 15 or 16 of the Immigration Act 2009 (these sections list certain persons not eligible for visas or entry permissions, including if the Minister of Immigration consider that person is or is likely to be a threat or risk to security).

14. Critical infrastructure issues were first considered in the context of the Act s6(a)

[REDACTED]

[REDACTED] New Zealand has specific restrictions on the foreign ownership of some companies (currently Air New Zealand Limited and Chorus Limited), and a generic overseas investment regime. s6(a)

[REDACTED]

<sup>2</sup> There are three investment types: Sensitive land, significant business assets, or fishing quota.

<sup>3</sup> The Cabinet paper can be accessed at

<http://www.treasury.govt.nz/publications/informationreleases/overseasinvestment/pdfs/cabmem-3mar08.pdf>

15. As a result, a new factor (regulation 28(h)) was added to the Overseas Investment Regulations 2005 (Regulations) on 4 March 2008 in assessing whether an overseas investment in sensitive land will or is likely to benefit New Zealand. Note - the vast majority of investments in sensitive land must meet the "benefit to New Zealand" criterion for consent to the investment to be granted. Regulation 28(h) reads:

*Whether the overseas investment will, or is likely to, assist New Zealand to maintain New Zealand control of strategically important infrastructure on sensitive land.*

16. The Act or the Regulations do not specify what the requisite level of New Zealand control should ideally be, and nor is "strategically important infrastructure" defined.
17. The introduction of the new regulation did not have the desired effect. This is because regulation 28(h), was at the time, was only one of 19 factors<sup>4</sup> that needed to be taken into account in assessing whether or not an investment was or was likely to benefit New Zealand. In addition, if the investment was of a different type (for example, a significant business asset investment), regulation 28(h) was not able to be considered as "benefit to New Zealand" is not a relevant criterion for this investment type. s6(a)

18. Subsequently, in the context of a review of the Act in 2009/2010, the Minister of Finance, Hon Bill English, sought advice from the Treasury for information about the use of a "substantial harm" test that would apply in addition to the "investor test" and (if applicable) the "benefit to New Zealand" test, along with a government policy statement on foreign investment. The "substantial harm" test would be applied at the Minister's discretion if he/she considered that the investment raises concerns that could not be addressed in other tests. The only change to the current benefit to New Zealand test would be to remove the "strategically important infrastructure" factor, as the "substantial harm" test would effectively supersede it as it would allow for assessment of similar issues. The remaining factors would not be changed.
19. It is noted that the example "substantial harm test" clause suggested by the Treasury in its report would be triggered when, in the Minister of Finance's view, "the investment will not, or is not likely to, result in substantial harm to New Zealand by threatening public order, public health and safety or essential security interests". This is a much narrower test than a "critical

<sup>4</sup> Since 2008, two additional factors have been added; there are currently 21 factors that need to be considered.



infrastructure" test. It was suggested by the Treasury that in declining an application under the substantial harm test, the Minister of Finance would have regard to a government policy statement, but presumably this statement would need to be consistent with, and not wider than, the "substantial harm test".

20. The Treasury advice does not appear to have been acted upon further.
21. On 13 January 2011, two new factors were added to the Regulations, regulations 28(i) and (j). Of relevance to this discussion is regulation 28(i), a new "economic interests" factor, which reads:
- 28(i) Whether New Zealand's economic interests will be adequately promoted by the overseas investment, including, for example, matters such as all or any of the following:
- (i) whether New Zealand will become a more reliable supplier of primary products in the future:
  - (ii) whether New Zealand's ability to supply the global economy with a product that forms an important part of New Zealand's export earnings will be less likely to be controlled by a single overseas person or its associates:
  - (iii) whether New Zealand's strategic and security interests are or will be enhanced:
  - (iv) whether New Zealand's key economic capacity is or will be improved.
22. According to the Minister of Finance's media release of 27 September 2010<sup>5</sup>, this new factor would allow ministers to consider whether New Zealand's economic interests are adequately safeguarded and promoted and would improve ministerial flexibility to respond to both current and future economic concerns about foreign investment, such as large-scale ownership of farmland.
23. The Minister of Finance also announced that the Government has also decided to retain the "strategically important infrastructure" factor. Although the Minister of Finance observed the test has not been used in the two years since it was introduced, on balance ministers concluded that removing it would reduce their flexibility in dealing with investment applications for sensitive land.
24. It will be noted that regulation 28 is expressed in the positive (i.e. if it can be demonstrated that New Zealand's economic interest will be adequately promoted, by, for example, showing that New Zealand's strategic and security interests are or will be enhanced), it will be counted as a benefit counting towards the "benefit to New Zealand" criterion. "Strategic and security interests" are not defined in the regulations.

<sup>5</sup> The comment refers to the fact that the "strategically important infrastructure" factor had not been the determining factor in declining an investment since the factor was introduced in March 2008.

25. The regulation 28(i) factor must be treated by the Overseas Investment Office (OIO), as the regulator, as being of high relative importance (compared to the other "non high relative importance" factors) under the 8 December 2010 Directive Letter<sup>6</sup>, but only if the investment involves large areas of farm land<sup>7</sup>. The Directive Letter only binds the regulator and does not bind the decision-making Ministers. The Act and the Directive Letter does not make it clear what the outcome is, if the factor is not relevant to the investment (or not met), and how the factor is weighed against other factors that are also rated as being of high relative importance. For example, if the factor is not met, it is not clear as to whether it is to be treated as neutral or negative.

s9(2)(a)



Catriona Robinson  
(for Howard Broad)  
Director, National Security Systems  
Security & Intelligence Group  
The Department of the Prime Minister & Cabinet

30 January 2015

<sup>6</sup> The Ministerial Directive Letter can be accessed at <http://www.linz.govt.nz/regulatory/overseas-investment/about-oio/legislation-ministers-delegated-powers>

<sup>7</sup> As defined in the Directive Letter (essentially the holding of farm land interests that are or will be of more than 10 times the average farm of that type)

## Appendix A: Critical Five Overview

### Overview

The Critical Five is a collaborative group focused on critical infrastructure protection. It was established in November 2012, and retains the founding members: Australia, Canada, New Zealand, United Kingdom and United States of America.

s6(a) The current chair is USA, and New Zealand will take over in mid-2015. It meets once a year face-to-face, hosted by the chair, and quarterly by teleconference.

s6(a)

s18(d)

Released under the Official Information Act 1982

Released under the Official Information Act 1982

s18(d)

Released under the Official Information Act 1982





**New Zealand Intelligence Community**  
*Te Rōpū Pārongo Tārehu o Aotearoa*

## Briefing Note

28 January 2015

**To** Hon Christopher Finlayson: Minister Responsible for GCSB; Minister in Charge of NZSIS

**From** Howard Broad, DCE: Security & Intelligence, DPMC

**For your** Information

**Subject** **Five Countries Ministerial: Session Four – Serious and Transnational Organised Crime**

### Purpose

1. This note briefs you on the s6(a) serious and transnational organised crime session of the upcoming Ministerial. It has been prepared by the Department of the Prime Minister & Cabinet drawing on information provided by Police, the Ministry of Justice, Customs, and the Department of Internal Affairs.

### Background

2. Those involved in transnational crime do not respect national borders and exploit gaps between national governments' information sharing and law enforcement systems. Determining opportunities to improve the exchange of relevant criminal history information to improve public security was a primary focus of the 2013 Five Country Ministerial (FCM). s6(a)

### Online Child Sexual Exploitation

*New Zealand's current work in this area*

3. New Zealand works closely with other countries and organisations, including Interpol, to locate offenders and identify victims of child exploitation both domestically and internationally.

4. A multi-agency approach is taken to this work, including sharing skills and resources. The main responsibilities and emphasis for each agency are:
  - **Police** – a focus on cases of physical and sexual abuse of children, online child exploitation, and also identifying child victims where Police actively investigates and infiltrates paedophile networks in conjunction with partner enforcement agencies;
  - **Customs** – a focus on identifying images of sexual abuse which are physically imported and exported on computers and other devices; and
  - the **Department of Internal Affairs (DIA)** – a focus on investigating image based offending, which is in large part internet-based.
5. In 2013, a formal multi-agency agreement was signed, outlining the way the three agencies work together in this area. New Zealand is seen as a world leader in the fight against child exploitation due, in part, to the high level of cooperation between the three agencies.

*The work of the Department of Internal Affairs' Censorship Compliance Unit (in conjunction with Police)*

6. DIA's Censorship Compliance Unit (the Unit) operates under a mandate provided by the Film, Videos, and Publications Classification Act 1993 (the Act). The Act prescribes a number of offences relating to the production, possession and distribution of objectionable material.
7. The Act also sets out the definition of objectionable material. This includes publications that promote or support, or tends to promote or support, the exploitation of children, or young persons, or both, for sexual purposes.

*Working with international agencies*

8. The DIA's Censorship officials have worked with Police to build strong relationships with international agencies. This allows officials to exchange information quickly and for efficient action to be taken to apprehend perpetrators. (A good recent example of cooperation between the US and New Zealand is included at Appendix A)
9. The Unit has a strong role in identifying victims in images of sexual abuse, both nationally and internationally. Officials from the DIA and the Police upload images to the Interpol International Child Sexual Exploitation Database to aid in the identification of victims.
10. DIA and Police contribute to Interpol's "worst-of list", which contains domains found to be distributing child sexual abuse material online. DIA is chair of two Interpol committees:
  - the Internet Facilitated Crimes Against Children Committee; and
  - the Internet Technical Working Group.



11. New Zealand Police is also interested in developing a formal working relationship with Europol, to allow for direct intelligence sharing and operational cooperation. Currently, New Zealand can only share intelligence with Europol through the Australian Federal Police.

*Operations to identify offenders*

12. DIA proactively runs operations, both nationally and internationally, to identify offenders. Investigations have resulted in overseas children being rescued and offenders located. Censorship staff track people sharing images of child sexual abuse on main communication platforms <sup>s6(c)</sup> [REDACTED].
13. For example, Operation Laminar identified over 50 key suspects in the worldwide distribution of child sexual abuse images, with some involved in the actual sexual abuse of the children depicted.
14. DIA provided evidence of the illegal activities to 20 countries and worked with United States authorities and Interpol. This enabled those countries' law enforcement agencies to take action against 55 people regarded as the top offenders in the trading of images.
15. The Operation started in October 2010, after the Unit found a significant number of child sexual abuse and exploitation images being exchanged via social network sites, including Facebook, Socialgo, and groups.

*Identifying victims*


16. Police, DIA and Customs work together, within their various fields of expertise, to identify the victims of child exploitation images. <sup>s6(c)</sup> [REDACTED]
17. Police also provides one of the two trainers for the International Child Sexual Exploitation database in the Oceania region. Police has deliver specialised victim identification training to Japanese, Vietnamese and Korean Police forces.

*The Digital Child Exploitation Filtering System*

18. DIA works in partnership with New Zealand Internet Service Providers (ISPs) by offering them use of the Digital Child Exploitation Filtering System (the System).
19. The System blocks access to known websites that contain child sexual abuse material. It is designed to assist in combating the trade in child sexual abuse material by making it more difficult for people to access identified objectionable material.

20. The system is voluntary for ISPs. At this time, over 90 per cent of New Zealand internet traffic is covered by the system. For mobile usage, this coverage is 100 per cent.
21. Frequently asked questions about the System are attached as Appendix B.
22. DIA also works to remove child abuse images from the internet by working with content providers such as Google and Microsoft to remove objectionable images from search engines.

s6(a), 6(b)(i)



#### **Data Sharing/Travel**

24. Police currently shares information on known child sex offenders both formally and informally with international counterparts, to the extent permitted in current legislation.
25. Police is one of the main members in the Violent Crimes Against Children International Taskforce (FBI lead) and is a member of the Virtual Global Taskforce which is taking a proactive approach to reducing online child abuse and other forms of transnational child sexual exploitation.
26. Police is currently seeking an amendment to the Policing Act 2008 through the Organised Crime and Anti-Corruption Bill (International information sharing framework attached at Appendix C) to provide Police with an express power to share information, including personal information and information about ongoing child exploitation investigations, with international counterparts. In addition to clarifying and strengthening current information sharing provisions, this will enable the Government to implement the Preventing and Combating Crime Agreement with the United States.
27. Police and the Department of Corrections are seeking legislation to enable the establishment of a Child Sex Offender Register by 1 July 2016. It is noted that the information contained on the register will not be publicly available. Police will be relying on the amendment to the Policing Act via the OCAC Bill to enable the sharing of the personal information contained on the register beyond that which NZ law currently allows.

s6(a)



s6(a)



s9(2)(a)



Catriona Robinson  
(for Howard Broad)  
Director, National Security Systems  
Security & Intelligence Group  
The Department of the Prime Minister & Cabinet

30 January 2015



## Appendix A: "Child sex abuse imagery 'disturbing'"

*From the Timaru Herald published on 23 January 2015*

Possessing and distributing thousands of "disturbing and offensive" child-sex images has resulted in a Timaru man being jailed for two years and eight months.

Keith Mervyn Perrin, 57, appeared in the Timaru District Court yesterday before Judge Joanna Maze on one representative charge each of possession of objectionable material and distribution of objectionable material.

The charges relate to offending between April 2013 and November 2013.

Perrin possessed 7376 child-sexual-abuse images, 450 of which were moving images, and distributed 221 child-sexual-abuse images depicting children aged 3 months to pre-teens.

Perrin appeared distraught at times during yesterday's sentencing. Family members in attendance shouted "we love you" as he was taken from the dock.

Maze said the offending was organised and systematic, and went on for a period of five to eight years before Perrin was caught.

"This is not a recent activity," she said.

Maze said the images depicted children with adult males and animals.

"The content of the images included bondage, bestiality, distress, full penetrative sexual activity and very young children.

"The images were disturbing and offensive and depicted serious trauma to the victims involved. Each of the images depicted involved a different child."

She said cases such as Perrin's represented the most vulnerable in a community and "we owe a duty of care to all children to protect them wherever they might be".

Yahoo and two United States organisations, including Homeland Security, helped to pinpoint Perrin's offending.

Perrin was referred to the Department of Internal Affairs after Yahoo detected objectionable image uploads to his Flickr account and referred them on to the National Centre for Missing and Exploited Children system in the United States, which, in turn, referred them to the department.

The judge said the aim of sentencing was to protect, deter and hold a person responsible.

"Sentences should reflect the damage done to the children involved," she said.

"The continued circulation and distribution of the images represents the ongoing victimisation of the children."

She said the impact on the children was likely to be lifelong.

Maze sentenced Perrin to two years and eight months' jail, and ordered the destruction of images and equipment seized.



## **Appendix B: Frequently asked questions - Digital Child Exploitation Filtering System**

### **What is the intention of the filter?**

The Digital Child Exploitation Filtering System has a very narrow purpose. It blocks access to known websites that contain child sexual abuse material.

It is one of the Department of Internal Affairs (DIA) measured responses to community expectations that the government and internet service providers (ISPs) should do more to provide a safe internet environment.

It is designed to assist in combating the trade in child sexual abuse material by making it more difficult for persons with a sexual interest in children to access that material.

It is also an educative tool to raise the public's awareness of this type of offending and the harm caused to victims.

The filtering system complements the information, education and enforcement activity undertaken by the Censorship Compliance Unit of.

DIA is working in partnership with New Zealand ISPs and offering them a choice to protect their customers from accessing these illegal websites inadvertently or otherwise.

It is not a magic bullet that will prevent everyone from accessing any sites that might contain images of child sexual abuse. But it is another important tool in the Department's operations to fight the sexual abuse of children.

### **How does it work?**

Using a secure link the system advertises to an Internet Service Provider routing information that relates to a list created by the Department of known websites that host child sexual abuse material.

When someone attempts to access an Internet Protocol (IP) address that matches this routing information, that request is sent to the DCEFS for examination.

If the request is for the URL of a known website, meaning it is currently within the list, the system will present a landing page informing the user that the request has been stopped.

If the URL does not match an item on the list the user's request is forwarded on.

### **Objections have been raised about the filter and the fact that ISPs are taking it up. Is this filter unique?**

No. According to a Statistics NZ survey in June 2009 21 per cent of ISPs offered some form of web content filtering as a free service.

ISPs would be considered remiss if they did not provide, for example, anti-spam filters.

### **What evidence is there that a filter such as this will have a material affect on reducing access to child pornography by offenders?**

A great deal of traffic goes to websites containing images of child sexual abuse. Websites play a part in transactions to purchase such images and act as a gateway to peer-to-peer services.

During DIA's two-year trial 1,055,277 requests for objectionable websites were refused (Note: these would have included repeated requests by individuals and "pop-ups and pop-under" where sites uninvited provide links to other objectionable material).

### **What is DIA's response to concerns that the filter impacts on the civil liberties of New Zealand internet users?**

DIA is concerned about the sexual abuse of children involved in the creation of the objectionable pictures. No one has the right to view illegal content that focuses on the sexual abuse of children; just as no one has a right to import illegal books and DVDs.

The filter will focus solely on websites offering clearly illegal, objectionable images of child sexual abuse.

It is a prevention tool, not a law enforcement tool and the anonymity of anyone who is blocked from accessing objectionable sites will be preserved.

The adults who make, trade or view these in New Zealand are parties to a serious offence. They contribute to an international market that supports and encourages further abuse.

The children who are victims of this activity sometimes suffer the psychological effects of their abuse for many years after the physical offending has ended.

Images that are distributed on the Internet never go away. With each download the person involved is re-victimised.

### **What assurances are there that the filter will not in future be extended to block content other than that intended?**

DIA's contract for the use of the software that supports the DCEFS constrains its use to filtering child sexual abuse material.

A Code of Practice has been put in place to govern the operation of the system and an Independent Reference Group (IRG) appointed to ensure the Department holds to its promise that the filter will focus solely on objectionable websites.

As the system advises people that they have been blocked, any departure from that stated aim would be widely publicised and participating ISPs would withdraw from using the system.

The fact that the system is voluntary provides an important further assurance that the system will keep to its stated purpose and that concerns about "scope creep" are unfounded. Should ISPs be concerned with the direction of the filtering system, they are able to withdraw.



## Appendix C: International Information Sharing Framework

- Framework provides Police with a broad power to share information, including personal information, with its international counterparts.
- The statute will provide that:
  - Police may share information with an overseas agency or body performing one or more of the functions set out in s9 of the Policing Act OR asset recovery.
  - That the information shared must be necessary for the overseas agency or body to discharge their s9 function(s) OR asset recovery.
  - The information may only be disclosed:
    - (i) With the consent of the individual concerned, or
    - (ii) Under a bilateral or multilateral Government agreement, or
    - (iii) In response to an Interpol request, or
    - (iv) Under an agency-to-agency agreement entered, or
    - (v) In response to a request being met by a specific NZ Police individual or business unit:
      - a. In accordance with approval given by the Police Commissioner, in consultation with the Privacy Commissioner, to specific individuals or business units (eg OCEANZ, OFCANZ, FIU, Electronic Crime Lab, Liaison Officers), and
      - b. Where guidelines (or Police Instructions) are in place to ensure appropriate sharing
- The Commissioner will need to consult with OPC in advance of finalising Agency to Agency Agreements.

### **Reporting**

Required to:

- Report annually to OPC on the operation of assurance processes to ensure that the statutory criteria for international information sharing are being adhered to (i.e. iii-v).
- Identify areas of risk and undertake a rolling cycle to review/audit the information sharing processes under iii-v.
- Make Agency to Agency Agreements publicly available, unless there is good reason under the OIA for withholding the agreement or parts of it.
- Make publicly available a list of which business units and individuals are authorised to share information internationally, unless there is good reason under the OIA for withholding the names or parts thereof.

s6(a)

Released under the Official Information Act 1982

Released under the Official Information Act 1982

**Joint FCM/Quintet Meeting**  
**February 16 and 17, 2016 ■ Washington, DC**



1	<b>Agenda</b>
2	<b>Session 1: Counter-terrorism and Information sharing for National Security</b> <ul style="list-style-type: none"> <li>• s6(a), 6(b)(i)</li> <li>• [REDACTED]</li> <li>• <b>Briefing Note: Session 1: Information Sharing and Counter-terrorism</b> (DPMC)</li> </ul>
3	<b>Session 2: Countering Violent Extremism</b> <ul style="list-style-type: none"> <li>• s6(a), 6(b)(i)</li> <li>• [REDACTED]</li> <li>• <b>Briefing Note: Session 2: Countering Violent Extremism</b>(DPMC)</li> </ul> <p><u>Background Reading</u></p> <ul style="list-style-type: none"> <li>• <i>New Zealand Gang Action Plan</i> (NZ Police)</li> <li>• <i>Whole-of-Government Action Plan to Reduce the Harms Caused by New Zealand Adult Gangs and Transnational Crime Groups</i> (NZ Police)</li> <li>• <i>WoG Gang Action Plan Programme Charter</i> (NZ Police)</li> </ul>
4	<b>Joint Lunch Day One:</b> s6(a), 6(b)(i) [REDACTED]
5	<b>Session 3: Cyber</b> <ul style="list-style-type: none"> <li>• <i>Cyber - Encryption</i> s6(a)</li> <li>• <b>Briefing Note: Session 3: Cyber: Encryption</b> s6(a)</li> </ul> <p><u>Background Reading</u></p> <ul style="list-style-type: none"> <li>• <b>Briefing Note: Cyber Security Issues</b> (DPMC)</li> <li>• <i>Summary of New Zealand's Cyber Security Strategy</i> (DPMC)</li> </ul>
6	<b>Session 4: Foreign Investment in Critical Infrastructure</b> <ul style="list-style-type: none"> <li>• s6(a), 6(b)(i)</li> <li>• <b>Briefing Note: Session 4: Presentation and Discussion of Foreign Investment</b> s6(a), 6(b)(i) (DPMC)</li> </ul>
7	<b>Joint Lunch Day Two:</b> s6(a), 6(b)(i) s6(a), 6(b)(i) [REDACTED]



# FIVE COUNTRY MINISTERIAL



**2016 Agenda**  
**16-17 February**  
**Washington, D.C.**

## **Tuesday 16 February: Joint Ministerial and Quintet Session**

Arrival from 0800

0815-0830      **Opening Remarks**

0830-0945

s6(a)

0945-1000

Coffee Break

1000-1130

**Session 1: Counterterrorism and Information Sharing for  
National Security**

s6(a)

1130-1140

Coffee Break

Out of scope

1145-1300

**Session 2: Countering Violent Extremism**

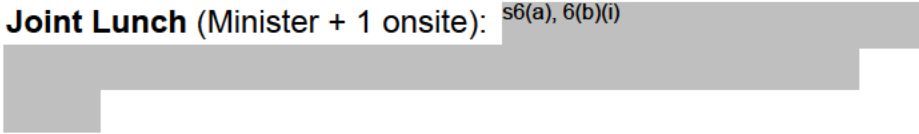
s6(a)

s6(a)



1300-1400

**Joint Lunch** (Minister + 1 onsite): s6(a), 6(b)(i)



1400-1415

**Group Photograph**

1415-1530

**Session 3: Cyber**

s6(a)



1530-1600

**Session 4: Foreign Investment in Critical Infrastructure**

s6(a)




1600-1615

**Closing Remarks**

1615-1745

**Bilateral Meetings and Refreshments**

Out of scope



1630-1700

1715-1745

1900 – 2100

**Joint Ministerial and Quintet Dinner** (Ministers – offsite)

*Reception begins at 1900*

*Dinner begins at 1930*

**Wednesday 17 February: Five Country Ministerial Session**

Arrival from 0800

0800-0845      **Coffee**

0815-0845      **Bilateral Meetings**

Out of scope

0850-0950

s6(a)

1000-1115

**Session 1: Information Sharing for National Security Screening  
Purposes**

s6(a)

1120-1135

**Coffee Break**

Out of scope

1140-1225

**Session 2: Visa Waiver and Trusted Traveler Programs**

s6(a)

s6(a)

1230-1245

**Closing Remarks**

1300-1400

**Joint Ministerial and Quintet Lunch** (Minister +1 onsite)  
**Enhanced Coordination of FVEY Activities to Include**  
**Discussion of Law Enforcement Encompassing Both Criminal**  
**Justice and Border Management Activities**

s6(a)

1400-1630

**Bilateral Meetings**

1415-1445

Out of scope

1500-1530

1545-1615



# Security Council

Distr.: General  
24 September 2014

## Resolution 2178 (2014)

**Adopted by the Security Council at its 7272nd meeting, on  
24 September 2014**

*The Security Council,*

*Reaffirming* that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever and by whomsoever committed, and *remaining* determined to contribute further to enhancing the effectiveness of the overall effort to fight this scourge on a global level,

*Noting with concern* that the terrorism threat has become more diffuse, with an increase, in various regions of the world, of terrorist acts including those motivated by intolerance or extremism, and *expressing* its determination to combat this threat,

*Bearing in mind* the need to address the conditions conducive to the spread of terrorism, and *affirming* Member States' determination to continue to do all they can to resolve conflict and to deny terrorist groups the ability to put down roots and establish safe havens to address better the growing threat posed by terrorism,

*Emphasizing* that terrorism cannot and should not be associated with any religion, nationality or civilization,

*Recognizing* that international cooperation and any measures taken by Member States to prevent and combat terrorism must comply fully with the Charter of the United Nations,

*Reaffirming* its respect for the sovereignty, territorial integrity and political independence of all States in accordance with the Charter,

*Reaffirming* that Member States must ensure that any measures taken to counter terrorism comply with all their obligations under international law, in particular international human rights law, international refugee law, and international humanitarian law, *underscoring* that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures, and are an essential part of a successful counter-terrorism effort and notes the importance of respect for the rule of law so as to effectively prevent and combat terrorism, and *noting* that failure to comply with these and other international obligations, including under the Charter



of the United Nations, is one of the factors contributing to increased radicalization and fosters a sense of impunity,

*Expressing grave concern* over the acute and growing threat posed by foreign terrorist fighters, namely individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict, and *resolving* to address this threat,

*Expressing* grave concern about those who attempt to travel to become foreign terrorist fighters,

*Concerned* that foreign terrorist fighters increase the intensity, duration and intractability of conflicts, and also may pose a serious threat to their States of origin, the States they transit and the States to which they travel, as well as States neighbouring zones of armed conflict in which foreign terrorist fighters are active and that are affected by serious security burdens, and *noting* that the threat of foreign terrorist fighters may affect all regions and Member States, even those far from conflict zones, and *expressing* grave concern that foreign terrorist fighters are using their extremist ideology to promote terrorism,

*Expressing concern* that international networks have been established by terrorists and terrorist entities among States of origin, transit and destination through which foreign terrorist fighters and the resources to support them have been channelled back and forth,

*Expressing* particular concern that foreign terrorist fighters are being recruited by and are joining entities such as the Islamic State in Iraq and the Levant (ISIL), the Al-Nusrah Front (ANF) and other cells, affiliates, splinter groups or derivatives of Al-Qaida, as designated by the Committee established pursuant to resolutions 1267 (1999) and 1989 (2011), *recognizing* that the foreign terrorist fighter threat includes, among others, individuals supporting acts or activities of Al-Qaida and its cells, affiliates, splinter groups, and derivative entities, including by recruiting for or otherwise supporting acts or activities of such entities, and *stressing* the urgent need to address this particular threat,

*Recognizing* that addressing the threat posed by foreign terrorist fighters requires comprehensively addressing underlying factors, including by preventing radicalization to terrorism, stemming recruitment, inhibiting foreign terrorist fighter travel, disrupting financial support to foreign terrorist fighters, countering violent extremism, which can be conducive to terrorism, countering incitement to terrorist acts motivated by extremism or intolerance, promoting political and religious tolerance, economic development and social cohesion and inclusiveness, ending and resolving armed conflicts, and facilitating reintegration and rehabilitation,

*Recognizing also* that terrorism will not be defeated by military force, law enforcement measures, and intelligence operations alone, and *underlining* the need to address the conditions conducive to the spread of terrorism, as outlined in Pillar I of the United Nations Global Counter-Terrorism Strategy (A/RES/60/288),

*Expressing* concern over the increased use by terrorists and their supporters of communications technology for the purpose of radicalizing to terrorism, recruiting and inciting others to commit terrorist acts, including through the internet, and



financing and facilitating the travel and subsequent activities of foreign terrorist fighters, and *underlining* the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law,

*Noting* with appreciation the activities undertaken in the area of capacity building by United Nations entities, in particular entities of the Counter-Terrorism Implementation Task Force (CTITF), including the United Nations Office of Drugs and Crime (UNODC) and the United Nations Centre for Counter-Terrorism (UNCCT), and also the efforts of the Counter Terrorism Committee Executive Directorate (CTED) to facilitate technical assistance, specifically by promoting engagement between providers of capacity-building assistance and recipients, in coordination with other relevant international, regional and subregional organizations, to assist Member States, upon their request, in implementation of the United Nations Global Counter-Terrorism Strategy,

*Noting* recent developments and initiatives at the international, regional and subregional levels to prevent and suppress international terrorism, and *noting* the work of the Global Counterterrorism Forum (GCTF), in particular its recent adoption of a comprehensive set of good practices to address the foreign terrorist fighter phenomenon, and its publication of several other framework documents and good practices, including in the areas of countering violent extremism, criminal justice, prisons, kidnapping for ransom, providing support to victims of terrorism, and community-oriented policing, to assist interested States with the practical implementation of the United Nations counter-terrorism legal and policy framework and to complement the work of the relevant United Nations counter-terrorism entities in these areas,

*Noting* with appreciation the efforts of INTERPOL to address the threat posed by foreign terrorist fighters, including through global law enforcement information sharing enabled by the use of its secure communications network, databases, and system of advisory notices, procedures to track stolen, forged identity papers and travel documents, and INTERPOL's counter-terrorism fora and foreign terrorist fighter programme,

*Having regard to and highlighting* the situation of individuals of more than one nationality who travel to their states of nationality for the purpose of the perpetration, planning, preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, and *urging* States to take action, as appropriate, in compliance with their obligations under their domestic law and international law, including international human rights law,

*Calling* upon States to ensure, in conformity with international law, in particular international human rights law and international refugee law, that refugee status is not abused by the perpetrators, organizers or facilitators of terrorist acts, including by foreign terrorist fighters,

*Reaffirming* its call upon all States to become party to the international counter-terrorism conventions and protocols as soon as possible, whether or not they are a party to regional conventions on the matter, and to fully implement their obligations under those to which they are a party,

*Noting* the continued threat to international peace and security posed by terrorism, and *affirming* the need to combat by all means, in accordance with the Charter of the United Nations, threats to international peace and security caused by terrorist acts, including those perpetrated by foreign terrorist fighters,

*Acting* under Chapter VII of the Charter of the United Nations,

1. *Condemns* the violent extremism, which can be conducive to terrorism, sectarian violence, and the commission of terrorist acts by foreign terrorist fighters, and *demand*s that all foreign terrorist fighters disarm and cease all terrorist acts and participation in armed conflict;

2. *Reaffirms* that all States shall prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents, *underscores*, in this regard, the importance of addressing, in accordance with their relevant international obligations, the threat posed by foreign terrorist fighters, and *encourages* Member States to employ evidence-based traveller risk assessment and screening procedures including collection and analysis of travel data, without resorting to profiling based on stereotypes founded on grounds of discrimination prohibited by international law;

3. *Urges* Member States, in accordance with domestic and international law, to intensify and accelerate the exchange of operational information regarding actions or movements of terrorists or terrorist networks, including foreign terrorist fighters, especially with their States of residence or nationality, through bilateral or multilateral mechanisms, in particular the United Nations;

4. *Calls upon* all Member States, in accordance with their obligations under international law, to cooperate in efforts to address the threat posed by foreign terrorist fighters, including by preventing the radicalization to terrorism and recruitment of foreign terrorist fighters, including children, preventing foreign terrorist fighters from crossing their borders, disrupting and preventing financial support to foreign terrorist fighters, and developing and implementing prosecution, rehabilitation and reintegration strategies for returning foreign terrorist fighters;

5. *Decides* that Member States shall, consistent with international human rights law, international refugee law, and international humanitarian law, prevent and suppress the recruiting, organizing, transporting or equipping of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, and the financing of their travel and of their activities;

6. *Recalls* its decision, in resolution [1373 \(2001\)](#), that all Member States shall ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice, and *decides* that all States shall ensure that their domestic laws and regulations establish serious criminal offenses sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offense:

(a) their nationals who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to

travel from their territories to a State other than their States of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training;

(b) the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to finance the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training; and,

(c) the wilful organization, or other facilitation, including acts of recruitment, by their nationals or in their territories, of the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training;

7. *Expresses* its strong determination to consider listing pursuant to resolution 2161 (2014) individuals, groups, undertakings and entities associated with Al-Qaida who are financing, arming, planning, or recruiting for them, or otherwise supporting their acts or activities, including through information and communications technologies, such as the internet, social media, or any other means;

8. *Decides* that, without prejudice to entry or transit necessary in the furtherance of a judicial process, including in furtherance of such a process related to arrest or detention of a foreign terrorist fighter, Member States shall prevent the entry into or transit through their territories of any individual about whom that State has credible information that provides reasonable grounds to believe that he or she is seeking entry into or transit through their territory for the purpose of participating in the acts described in paragraph 6, including any acts or activities indicating that an individual, group, undertaking or entity is associated with Al-Qaida, as set out in paragraph 2 of resolution 2161 (2014), provided that nothing in this paragraph shall oblige any State to deny entry or require the departure from its territories of its own nationals or permanent residents;

9. *Calls upon* Member States to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee established pursuant to resolutions 1267 (1999) and 1989 (2011) ("the Committee"), and further *calls upon* Member States to report any such departure from their territories, or such attempted entry into or transit through their territories, of such individuals to the Committee, as well as sharing this information with the State of residence or nationality, as appropriate and in accordance with domestic law and international obligations;

10. *Stresses* the urgent need to implement fully and immediately this resolution with respect to foreign terrorist fighters, *underscores* the particular and urgent need to implement this resolution with respect to those foreign terrorist fighters who are associated with ISIL, ANF and other cells, affiliates, splinter groups or derivatives of Al-Qaida, as designated by the Committee, and *expresses* its

readiness to consider designating, under resolution 2161 (2014), individuals associated with Al-Qaida who commit the acts specified in paragraph 6 above;

#### *International Cooperation*

11. *Calls upon* Member States to improve international, regional, and subregional cooperation, if appropriate through bilateral agreements, to prevent the travel of foreign terrorist fighters from or through their territories, including through increased sharing of information for the purpose of identifying foreign terrorist fighters, the sharing and adoption of best practices, and improved understanding of the patterns of travel by foreign terrorist fighters, and for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law;

12. *Recalls* its decision in resolution 1373 (2001) that Member States shall afford one another the greatest measure of assistance in connection with criminal investigations or proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings, and *underlines* the importance of fulfilling this obligation with respect to such investigations or proceedings involving foreign terrorist fighters;

13. *Encourages* Interpol to intensify its efforts with respect to the foreign terrorist fighter threat and to recommend or put in place additional resources to support and encourage national, regional and international measures to monitor and prevent the transit of foreign terrorist fighters, such as expanding the use of INTERPOL Special Notices to include foreign terrorist fighters;

14. *Calls upon* States to help build the capacity of States to address the threat posed by foreign terrorist fighters, including to prevent and interdict foreign terrorist fighter travel across land and maritime borders, in particular the States neighbouring zones of armed conflict where there are foreign terrorist fighters, and *welcomes* and *encourages* bilateral assistance by Member States to help build such national capacity;

#### *Countering Violent Extremism in Order to Prevent Terrorism*

15. *Underscores* that countering violent extremism, which can be conducive to terrorism, including preventing radicalization, recruitment, and mobilization of individuals into terrorist groups and becoming foreign terrorist fighters is an essential element of addressing the threat to international peace and security posed by foreign terrorist fighters, and *calls upon* Member States to enhance efforts to counter this kind of violent extremism;

16. *Encourages* Member States to engage relevant local communities and non-governmental actors in developing strategies to counter the violent extremist narrative that can incite terrorist acts, address the conditions conducive to the spread of violent extremism, which can be conducive to terrorism, including by empowering youth, families, women, religious, cultural and education leaders, and all other concerned groups of civil society and adopt tailored approaches to countering recruitment to this kind of violent extremism and promoting social inclusion and cohesion;

17. *Recalls* its decision in paragraph 14 of resolution 2161 (2014) with respect to improvised explosive devices (IEDs) and individuals, groups, undertakings and entities associated with Al-Qaida, and *urges* Member States, in this context, to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources, including audio and video, to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law;

18. *Calls upon* Member States to cooperate and consistently support each other's efforts to counter violent extremism, which can be conducive to terrorism, including through capacity building, coordination of plans and efforts, and sharing lessons learned;

19. *Emphasizes* in this regard the importance of Member States' efforts to develop non-violent alternative avenues for conflict prevention and resolution by affected individuals and local communities to decrease the risk of radicalization to terrorism, and of efforts to promote peaceful alternatives to violent narratives espoused by foreign terrorist fighters, and *underscores* the role education can play in countering terrorist narratives;

*United Nations Engagement on the Foreign Terrorist Fighter Threat*

20. *Notes* that foreign terrorist fighters and those who finance or otherwise facilitate their travel and subsequent activities may be eligible for inclusion on the Al-Qaida Sanctions List maintained by the Committee pursuant to resolutions 1267 (1999) and 1989 (2011) where they participate in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of, Al-Qaida, supplying, selling or transferring arms and related materiel to, or recruiting for, or otherwise supporting acts or activities of Al-Qaida or any cell, affiliate, splinter group or derivative thereof, and *calls upon* States to propose such foreign terrorist fighters and those who facilitate or finance their travel and subsequent activities for possible designation;

21. *Directs* the Committee established pursuant to resolution 1267 (1999) and 1989 (2011) and the Analytical Support and Sanctions Monitoring Team, in close cooperation with all relevant United Nations counter-terrorism bodies, in particular CTED, to devote special focus to the threat posed by foreign terrorist fighters recruited by or joining ISIL, ANF and all groups, undertakings and entities associated with Al-Qaida;

22. *Encourages* the Analytical Support and Sanctions Monitoring Team to coordinate its efforts to monitor and respond to the threat posed by foreign terrorist fighters with other United Nations counter-terrorism bodies, in particular the CTITF;

23. *Requests* the Analytical Support and Sanctions Monitoring Team, in close cooperation with other United Nations counter-terrorism bodies, to report to the Committee established pursuant to resolutions 1267 (1999) and 1989 (2011) within 180 days, and provide a preliminary oral update to the Committee within 60 days, on the threat posed by foreign terrorist fighters recruited by or joining ISIL, ANF and all groups, undertakings and entities associated with Al-Qaida, including:

(a) a comprehensive assessment of the threat posed by these foreign terrorist fighters, including their facilitators, the most affected regions and trends in radicalization to terrorism, facilitation, recruitment, demographics, and financing; and

(b) recommendations for actions that can be taken to enhance the response to the threat posed by these foreign terrorist fighters;

24. *Requests* the Counter-Terrorism Committee, within its existing mandate and with the support of CTED, to identify principal gaps in Member States' capacities to implement Security Council resolutions 1373 (2001) and 1624 (2005) that may hinder States' abilities to stem the flow of foreign terrorist fighters, as well as to identify good practices to stem the flow of foreign terrorist fighters in the implementation of resolutions 1373 (2001) and 1624 (2005), and to facilitate technical assistance, specifically by promoting engagement between providers of capacity-building assistance and recipients, especially those in the most affected regions, including through the development, upon their request, of comprehensive counter-terrorism strategies that encompass countering violent radicalization and the flow of foreign terrorist fighters, recalling the roles of other relevant actors, for example the Global Counterterrorism Forum;

25. *Underlines* that the increasing threat posed by foreign terrorist fighters is part of the emerging issues, trends and developments related to resolutions 1373 (2001) and 1624 (2005), that, in paragraph 5 of resolution 2129 (2013), the Security Council directed CTED to identify, and therefore merits close attention by the Counter-Terrorism Committee, consistent with its mandate;

26. *Requests* the Committee established pursuant to resolutions 1267 (1999) and 1989 (2011) and the Counter-Terrorism Committee to update the Security Council on their respective efforts pursuant to this resolution;

27. *Decides* to remain seized of the matter.

---



**New Zealand Intelligence Community**  
*Te Rōpū Pārongo Tārehu o Aotearoa*

## Briefing Note

12 February 2016

**To** Hon Christopher Finlayson: Minister in Charge of NZSIS; Minister Responsible for GCSB

**From** Howard Broad, Deputy Chief Executive, Security & Intelligence, DPMC

**For your** Information

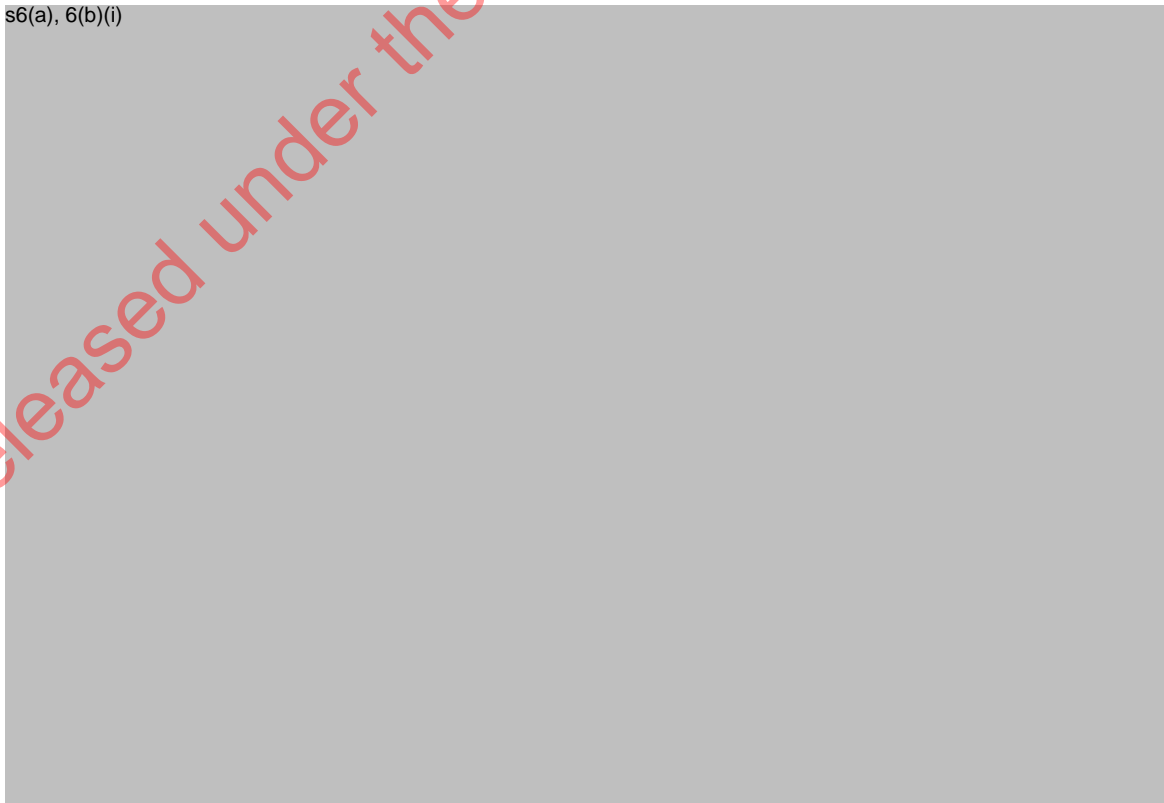
**Subject** Five Country Ministerial: Session 1: Counterterrorism and Information Sharing for National Security

## Purpose

1. This briefing provides you information to support your participation in the Five Country Ministerial (FCM) session on Counterterrorism and Information Sharing for National Security.

## Background


s6(a), 6(b)(i)







s6(a), 6(b)(i)



4. The topics covered in this session are closely related to those which will be covered in session 1 of day two of the FCM on Wednesday 17 February.

**Sharing of terrorism and watchlist information with border, transportation security and immigration officials**

5. New Zealand takes a case-by-case approach to sharing watchlist information. A risk based approach is taken to using it as part of the visa process, however all border movements are checked against it.

s6(a)



12. Legislation such as the Privacy Act regulates the sharing of information between agencies, and may limit it in some cases.

## Screening of refugees and asylees

s6(a)


### Sharing information on international air travel

18. Domestically, agencies operate closely with each other at the border and can access systems like CUSMOD (Customs modernisation system) and JBMS (Joint Border Management System) regarding border alerts. The 2014 Countering Terrorist Fighters Legislation Bill clarified that Police and other agencies could access CUSMOD for counter terrorism purposes.

19. Border agencies have their own ways that they talk to counterparts, including APP and similar systems. Much of this has evolved to deal with far broader issues than terrorism, for example compliance with visa and passport policy, and international agreements such as the Chicago Convention on Civil Aviation.

20. Passenger Name Record (PNR) data is collected by New Zealand Customs Service and retrieved by INZ on an as requested basis. PNR data is used to electronically profile passengers coming to New Zealand. It also provides details on connecting flights and travel routes.

s6(a), 6(b)(i)



**Supporting the Global Counterterrorism Forum (GCTF), Global Coalition to Counter ISIL/Da'esh (GCCCI) and United Nations (UN) efforts on foreign terrorist fighters (FTF)**

23. The 2014 Countering Terrorist Fighters Legislation Bill sought to address the issue of FTF. New Zealand also plays an important role in combating terrorism worldwide through a number of for a and contributions to the fight against ISIL.

s6(a)





s6(a)



## Recommendations

It is recommended that you:

1	Note	the content of this briefing	Yes/No
---	------	------------------------------	--------

Howard Broad  
Deputy Chief Executive, Security and Intelligence

DPMC

Hon Christopher Finlayson  
Minister in Charge of NZSIS  
Minister Responsible for GCSB

/ /2016



**New Zealand Intelligence Community**  
*Te Rōpū Pārongo Tārehu o Aotearoa*

## Briefing Note

15 February 2016

**To** Hon Christopher Finlayson: Minister in Charge of NZSIS; Minister Responsible for GCSB

**From** Howard Broad, Deputy Chief Executive, Security & Intelligence, DPMC

**For your** Information

**Subject** Five Country Ministerial: Session 2: Countering Violent Extremism

## Purpose

1. This briefing provides you information to support your participation in the Five Country Ministerial (FCM) session on Countering Violent Extremism (CVE).

## Background

2. A summary of New Zealand's key CVE initiatives since the last FCM is attached to the CVE working group paper that will be discussed at the meeting. A key theme of New Zealand's summary is that while we have specific CVE initiatives, community strengthening plays a key role in addressing conditions that may foster violent extremism.

3. In addition to a low level terrorism threat level we are fortunate to have low levels of extremism generally; it's not just that we don't have large terror networks but also don't have the harbouring communities in which they can thrive.


s6(a), 6(b)(i)





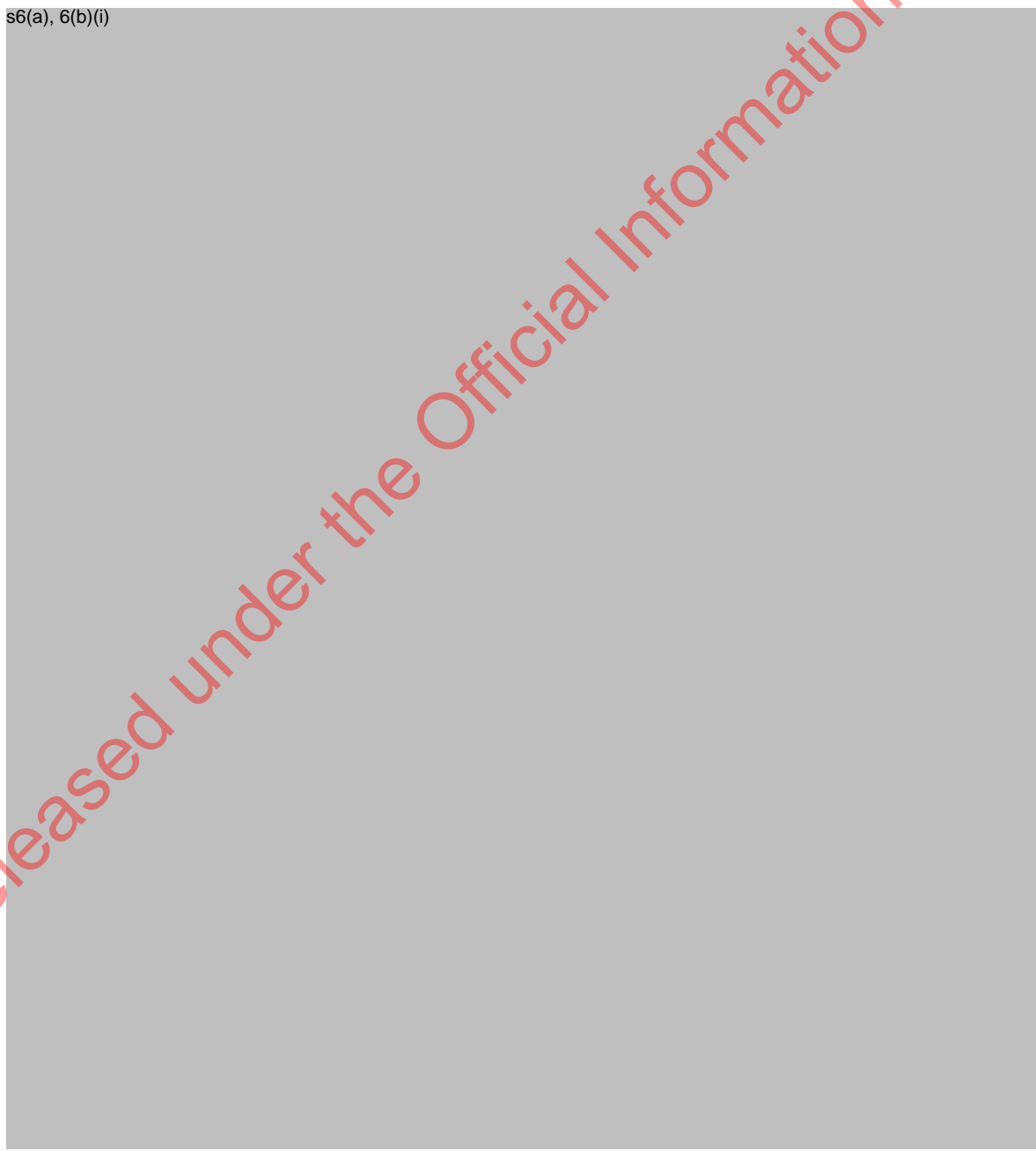
### Community cohesion and engagement

s6(a), 6(b)(i)



6. This type of work is closely aligned with New Zealand's current community strengthening approach and is highlighted in New Zealand's summary paper. Examples of this Office of Ethnic Communities and Ministry of Social Development community initiatives alongside the community engagement work of the New Zealand Police.

s6(a), 6(b)(i)



Released under the Official Information Act 1982



s6(a), 6(b)(i)

14. Government as well as industry and civil society have a critical role to play in countering extremism online. New Zealand is concerned by 'terrorist use of the Internet' to raise funds and spread propaganda. Of course, responses to such activity must be balanced with the need to respect human rights including freedom of expression, and this would be explored further during the course of this work.

## Recommendations

It is recommended that you:

1	Note	the content of this briefing	Yes/No

Howard Broad  
Deputy Chief Executive, Security and Intelligence

DPMC

Hon Christopher Finlayson  
Minister in Charge of NZSIS  
Minister Responsible for GCSB

/ /2016



---

# NEW ZEALAND GANG ACTION PLAN



**A long-term plan to address a complex issue, stopping the intergenerational grip gang life has on families, and to reducing victims at home and in our communities.**

### Did you know?

**APPROXIMATELY**  
**5,900**  
**CHILDREN**

---

can be linked to adult gang members via a parent-child relationship in the Child Youth and Family computer system.

**60%**  
**OF THOSE CHILDREN**

---

had a substantiated finding of abuse or neglect. Multiple findings were common.\*

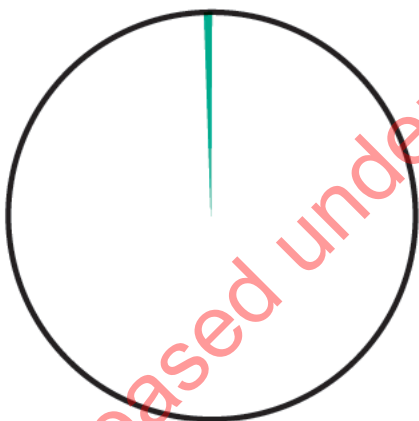
**ALMOST** **1/4**  
**OF CHILDREN OF GANG MEMBERS**

---

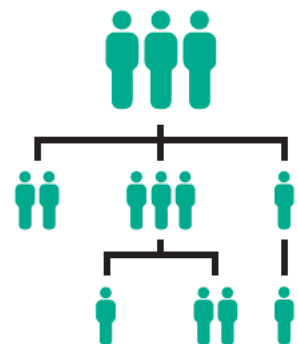
are known to the youth justice system.\*

**THE TOTAL COST TO POLICE OF THE 141,000 CHARGES LAID AGAINST GANG MEMBERS BETWEEN 1993–2012 IS \$241 MILLION.**

Charges included drugs, violence, sexual offences, anti-social, dishonesty, failure to answer bail.



GANG MEMBERS AND PROSPECTS MAKE UP LESS THAN 0.1% OF NZ POPULATION, BUT CREATE DISPROPORTIONATE HARM



---

Gang members and prospects are over-represented in family violence, child abuse and neglect, serious criminal offending, drug crime and imprisonment, and benefit dependency.

---

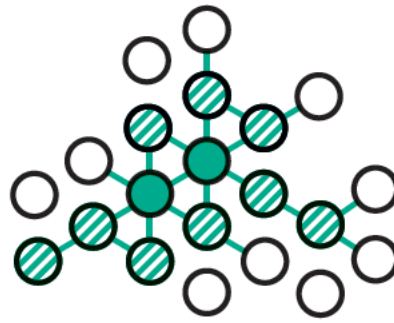
**AN INTER-GENERATIONAL PROBLEM**

---

## WHAT DOESN'T WORK



NZ and international experience shows single-focus enforcement or social intervention approaches don't work long-term.



Gangs adapt and expand.



It's a complex problem spanning social, economic and justice issues.

---

**Issues are complex, diverse and can't be fixed by one agency alone.**

---

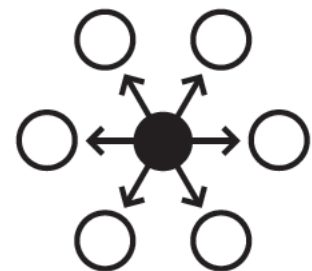
## A NEW APPROACH TO BREAK THE CYCLE – GANG ACTION PLAN



Gang Action Plan brings agencies together to share information and deliver a spectrum of enforcement and social interventions.



Aim is to encourage change in gang families and the community, while disrupting criminal networks and profits derived from offending.

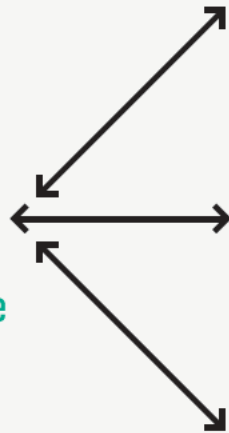


Actions delivered through existing programmes by informing a focused, whole-of-government, intelligence-led approach.

---

## FOUR ELEMENTS OF THE GANG ACTION PLAN

### GANG ACTION PLAN



### SOCIAL INITIATIVES

Improve intergenerational social results for those associated with gangs.



### TASKFORCES

Target drug trafficking and focus on criminal asset recovery.  
Target proceeds of crime.



### LEGISLATIVE TOOLKIT

Enhance multi-agency law enforcement.

### GANG INTELLIGENCE CENTRE

Produce combined intelligence to support the three action plan initiatives.

## INFORMATION SHARING



### PARTNER AGENCIES



The Gang Intelligence Centre is funded for two years initially.

Gang Action Plan progress will be tracked and measured to assess the impact of actions and interventions.

*This Cabinet Paper (21 pages) publicly available on the NZ Police website at:*

<https://www.police.govt.nz/about-us/publication/cabinet-paper-whole-government-action-plan-reduce-harms-caused-new-zealand>

s18(d)

Released under the Official Information Act 1982

# Programme Charter

---

**Whole of Government**

**Gang Action Plan**

**September 2015**

**V0.5**

Released under the Official Information Act 1982



## Whole of Government Gang Action Plan

### Version Release History

Release	Status	Date	Author	Description of Release
V0.1	Draft	May 2015	Louise Collins	Initial draft
V0.2	Draft	July 2015	Louise Collins	Draft for workstream review
V0.3	Draft	August 2015	Louise Collins	Draft for workstream review
V0.4	Draft	August 2015	Louise Collins	Draft for all agency review
V0.5	Draft	September 2015	Louise Collins	Draft for Steering Group review

This Programme Charter is to be signed off at the Whole of Government Gangs Action Plan Steering Group meeting in October 2015. Any required changes will be noted in the minutes.



# 1 CONTENTS

<b>1. Introduction.....</b>	<b>4</b>
1.1 Adult Gang Definition.....	4
1.2 Background .....	4
<b>2. Programme Aims .....</b>	<b>5</b>
<b>3. Governance .....</b>	<b>6</b>
<b>4. Programme Initiatives .....</b>	<b>8</b>
4.1 Gang Intelligence Centre .....	8
4.2 Start at Home .....	9
4.3 Dedicated Taskforces .....	9
4.4 Legislative Toolkit .....	10
<b>5. Programme Management.....</b>	<b>11</b>
5.1 Performance Framework .....	11
5.2 Communications.....	11
5.3 Information Sharing .....	11
5.4 Programme Implementation .....	11
<b>6. Timing and Costs.....</b>	<b>12</b>
6.1 Costs .....	12
6.2 Timing.....	12
<b>7. Related Initiatives .....</b>	<b>13</b>
7.1 Building on existing initiatives .....	13

## 1. Introduction

The Whole of Government Action Plan aims to reduce the harms caused by New Zealand Adult Gangs and Transnational crime groups. This includes harm to immediate family, extended family and associates as well as to the community.

New Zealand has a complex gang problem that spans social, economic and justice issues. Adult gangs and transnational crime groups create disproportionate harm in New Zealand. While overall crime is trending downwards, serious offending by adult gang members increased by 15 percent in 2013. Almost half of the serious offences committed by gang members are family violence related. A high proportion of gang members' children experience multiple incidents of abuse or neglect. Historical enforcement responses to adult gangs and transnational crime groups have produced successful operations, but these groups have continued to expand and adapt.

### 1.1 Adult Gang Definition

A New Zealand Adult Gang is an organisation, association or group with the following characteristics: a common name; one or more common identifiers; and whose members or associates either individually or collectively promote, encourage or engage in criminal activity that is driven by a desire for profit and/or to create an atmosphere of fear and intimidation, which is enabled by virtue of membership in the gang.

### 1.2 Background

New Zealand's historical response to adult gangs has been focused mainly on criminal offending rather than social harms. Previous responses have involved individual agencies trying to tackle specific issues in isolation, such as the manufacture and supply of drugs or establishing work schemes. While there have been successful operations targeting outlaw motorcycle gangs and transnational crime groups, these groups have continued to expand and adapt. Ethnic gangs of New Zealand origin continue to expand through intergenerational membership.

New Zealand has been moving towards a multi-agency approach to criminal offending by adult gangs and transnational crime groups through the All-of-Government Response to Organised Crime and the Organised and Financial Crime Agency New Zealand. These approaches target high-level criminal offending by organised crime groups, specifically targeting bribery and corruption, money-laundering and international financial transactions. Their scope however does not treat the social issues of gang membership or criminal offending.

In June 2013, the Cabinet Strategy Committee (STR) invited the Minister of Police, in consultation with other relevant Ministers (including Social Sector Ministers), to report back to the Cabinet Social Policy Committee (SOC) in due course with:

- high-level proposals that will make a real difference in reducing the influence of gangs in New Zealand; and
- recommendations on a proposed fusion centre that would enable agencies to combine intelligence to allow better targeting and co-ordinating activities focused on gangs.

In June 2014 a paper proposing the Whole-of-Government Gangs Action Plan was presented to the Cabinet Social Policy Committee (SOC) by the Minister of Police and was accepted with all recommendations noted or agreed.

This Programme Charter draws extensively on wording from that Cabinet Paper.

## 2. Programme Aims

The objective of the Gangs Action Plan is to produce the outcome result of a reduction in harm to society, caused by adult and transnational gang members, by combining enforcement and social intervention activity.

The aims of the Gangs Action Plan programme are:

1. To achieve the outcomes of the June 2014 Cabinet paper. This includes the delivery of actions relating to the four initiatives of Gang Intelligence Centre, Start at Home, Dedicated Taskforces and the Legislative Toolkit.
2. To support the Cabinet paper initiatives by the development of a two tiered approach to social intervention with both system level changes and place based initiatives.

The Cabinet Paper states that “most actions are intended to be delivered through existing programmes” and thus the programme will achieve its aims by integrating and extending existing programmes rather than through the development of new services. Where new operating systems and processes are identified that enable better alignment of agency services to achieve the programmes goals, these will be considered for implementation.

Released under the Official Information Act 1982

### 3. Governance

Governance and oversight of the development and implementation of the action plan work programme is provided by the Inter Agency Governance steering Group. This group also provides support to the Programme Manager and work stream leads.

The Steering Group acts as a gateway to the Social Sector Forum and Ministerial Advisory Group which meets quarterly. Report backs are channelled to Ministers and the Cabinet SOC where necessary on the achievement of milestones directed by the 2014 Cabinet paper.

The Steering Group is comprised of representatives from government agencies involved, as follows:

Steering Group Representatives	
Chair - Deputy Commissioner National Operations (NZ Police)  Agency representatives at DCE level or as nominated: <ul style="list-style-type: none"> <li>• Social Development</li> <li>• Justice</li> <li>• Corrections</li> <li>• Te Puni Kokiri</li> <li>• Internal Affairs</li> <li>• Inland Revenue</li> <li>• Department of Prime Minister and Cabinet</li> <li>• Customs</li> <li>• Immigration</li> <li>• Education</li> <li>• Health</li> </ul>	Work Stream Project leads x 4  <u>Police:</u> <ul style="list-style-type: none"> <li>• Programme Manager</li> <li>• GM: Maori Pacific Island Ethnic Services</li> <li>• Assistant Commissioner International, Intelligence &amp; Investigations</li> </ul>

The Steering Group will act collaboratively and constructively to ensure work programme initiatives are prioritised, resourced and supported to achieve their purpose. Key activities fall within the following areas, with details documented in the Gangs Action Plan Steering Group Terms of Reference:

- Reporting
- Communications
- Inter-agency collaboration
- Risk Management
- Funding and resource allocation

The governance and reporting structure for the Gangs Action Plan is portrayed in the diagram below:

## Whole of Government Gang Action Plan



## 4. Programme Initiatives

The whole-of-government action plan comprises four initiatives. These initiatives directly address the different motivators and harms, are designed to improve our knowledge of and response to gangs, improve across-government coordination of service delivery and deliver a more effective law enforcement approach. These are:

- the creation of a multi-agency **Gang Intelligence Centre** to provide a combined intelligence picture of gang activity, inform decision making on preventative, investigative and enforcement interventions, and identify vulnerable children, youth and gang family members for social service support
- **Start at Home**: a programme of social initiatives to support gang members and their families to turn away from the gang lifestyle, and reduce the likelihood of young people joining gangs
- establishment of two multi-agency **Dedicated Enforcement Taskforces**: one to strengthen border protection to target drug trafficking networks and restrict international gang travel, and one to strengthen asset recovery efforts and prevent and target financing of crime and profit received from crime
- work to ensure that the **Legislative Toolkit** enables law enforcement agencies to appropriately target cash acquired illegally, better detect, investigate and prosecute organised crime, monitor gang offenders on release from prison, and manage risk to keep communities safe.

### 4.1 Gang Intelligence Centre

The Gang Intelligence Centre will deliver intelligence product focused on enhancing the understanding of the New Zealand Adult Gang environment to inform prevention, intervention and enforcement activity; to reduce harm and improve social and economic outcomes. It will be primarily be focused on producing intelligence reporting to support the three other Action Plan initiatives (Start at Home, Dedicated Taskforces and the Legislative Toolkit) but its scope and purpose allows for other agency initiatives and business-as-usual activities as prioritised according to the Gangs Action Plan decision Making Framework. Therefore, Gang Intelligence Centre analysis will span a wide range of issues and problems. Through supporting the work of the Dedicated Taskforces, the Gang Intelligence Centre will need to analyse a wide range of offending, both domestic and transnational in nature. Conversely, intelligence product and analysis in support of the Start at Home programme will require a focus on improving social results for gang members and their families, by taking an inter-generational approach to data collection and analysis.

It is expected the Gang Intelligence Centre will produce tactical, operational and strategic intelligence products informed by a wide range of agency information and intelligence. Specifically, intelligence product will focus on New Zealand Adult Gang offenders (including their networks and enablers), their victims and those linked to gangs (families and children for example). This work will be driven by enforcement requirements as well as providing intelligence and analysis to help improve inter-generational social results for gangs-linked cohorts as part of the Gangs Action Plan.

Initially the Gangs Intelligence Centre will involve the following seven agencies, who make up the Working Group:

- Police
- Ministry of Social Development
- Department of Corrections
- MBIE - Immigration

- Inland Revenue
- Department of Internal Affairs
- New Zealand Customs Service.

The Cabinet mandate for the Whole of Government Action Plan lists the Accident Compensation Corporation, the Ministry of Housing, the Ministry of Health and the Ministry of Education as agencies that are to be involved in the second phase of the Gang Intelligence Centre.

## 4.2 Start at Home

The Start at Home programme is targeted towards achieving sustainable reductions in harm by having initiatives that address the intergenerational nature of ethnic adult and youth gangs. The initiatives within the programme work with gang families and young people to:

- help young people at risk of joining gangs reach their potential outside of a gang;
- provide alternatives to gang lifestyle for gang-connected families;
- reduce victimisation and violence in gang families and;
- build resilience in communities with a large gang presence.

Start at Home provides an intervention point across existing initiatives intended to protect vulnerable children, reduce family violence, improve educational achievement, improve educational outcomes, and improve health outcomes for the most vulnerable. This will ensure that those individuals and families who are least likely to engage can access services and that agencies can directly connect with these individuals.

Start at Home is primarily targeting indigenous ethnic gangs (as opposed to outlaw motorcycle gangs and transnational crime groups). Indigenous ethnic gangs mainly comprise dysfunctional, inter-generational family groups. These gangs are predominantly Māori and have strong geographic ties to certain locations. Indigenous ethnic gang membership is strongly connected with poor social and economic outcomes, including low rates of educational achievement, poor health outcomes and high rates of unemployment and child abuse and / or neglect. These poor social outcomes are coupled with high rates of criminal offending, including retaliatory offending between gangs and family violence.

The first phase of Start at Home is Police lead and will include delivery of the Summer Night Lights programme, safety planning for women who are victims of intimate partner violence, replication of the gang women's community garden concept in Gisborne, and reintegration programmes for gang members on release from prison.

The second phase of Start at Home will include delivery of programmes by MSD, Corrections and Health to cover the four areas of:

- Reduced intergenerational gang involvement.
- Improved outcomes for children of gang members who are in prison.
- Improved access and services to treat mental health, drug and alcohol problems.
- Skills and employment programmes – particularly for youth.

## 4.3 Dedicated Taskforces

The dedicated taskforces initiative involves the establishment of two taskforces. One of these taskforces is titled the Outlaw Motorcycle Gang Border Protection Taskforce. The aim of the taskforce is to strengthen border protection to target drug trafficking networks and restrict international gang travel. This is to be achieved through better coordination of activities to stop new gangs entering New Zealand, prevent the spread of existing gangs and protect New Zealand from the trafficking of drugs, arms and other illegal



commodities. Part 1 will involve Police, Customs and the Immigration arm of the Ministry of Business, Innovation and Employment and part 2 will seek to explore opportunities to involve international counterparts.

The other taskforce is titled the Criminal Asset Confiscation Taskforce. The aim of that taskforce is to strengthen asset recovery efforts and prevent and target financing of crime and profit received from crime. This will enable flexible and timely joint criminal proceeds recovery action and prevent and target financing of crime and profit received from crime. Part 1 will involve Inland Revenue and Police and Part 2 will explore opportunities to involve the Department of Internal Affairs and the Ministry of Business Innovation and Employment.

#### 4.4 Legislative Toolkit

The legislative toolkit initiative incorporates investigation of legislative options in the following areas:

Part 1:

1. Firearm Prohibition Orders
2. Interim freezing orders
3. Interim freeing power (cash found in suspicious circumstances)
4. Use of unexplained wealth laws in other jurisdictions
5. GPS monitoring of gang offenders on release from prison

Part 2:

6. Investigate opportunities to pilot drug detector dogs at domestic ports (maritime and air) to prevent and disrupt drug trafficking between the North and South Islands
7. Enhanced protection for Police Officers deployed in covert operations
8. Tax Administration Act amendment explicitly enabling IR to share business entity information

## **5. Programme Management**

### **5.1 Performance Framework**

Police will work with agencies to develop a performance management framework as part of the implementation of the action plan. Specific measures will be developed that feed directly into Better Public Service result areas to boost skills and employment, protect vulnerable children and reduce crime.

### **5.2 Communications**

A multi agency communications strategy and plan will be required to provide key messages and planned engagement with Ministers, internal agencies and the public.

### **5.3 Information Sharing**

There are legal, technical and agency policy issues for information and intelligence sharing that are governed in the first instance by the Privacy Act but also other legislation applicable to each agency. The Gangs Action Plan must ensure that there is a suitable plan for sharing information and intelligence that ideally does not require legislative change and that involves a minimum of complex undertaking such as Agreed Information Sharing Agreements and Memorandums of Understanding.

### **5.4 Programme Implementation**

The intent of the Gangs Action Plan is to reduce the way Gangs impact negatively on the community by using effective targeted social interventions together with enforcement. Gangs and their families are likely to require intensive interventions that will involve government agencies, service providers and gang families working together to achieve sustainable long term goals. New approaches, systems and ways of working together will be required and allowed for during implementation.

## 6. Timing and Costs

### 6.1 Costs

Most actions are intended to be delivered through existing programmes. Funding proposals may be developed for some activities that cannot be delivered through existing programmes or within baseline. A funding bid to the Justice Sector Fund was successful in obtaining funding for the Gangs Intelligence Centre over two years to enable the Centre to develop and embed its systems, and demonstrate its value to contributing agencies and the wider group of potential contributors to deliver Better Public Service targets.

All other initiatives are to be delivered within baseline using existing resourcing.

### 6.2 Timing

The action plan will be implemented in two parts. Part one actions will be implemented by December 2015, with the exception of the proposed legislative amendments which depend on completing the policy work and the parliamentary process. Part two actions are being developed and will be implemented at a later date with timeframes identified through the design stage which commenced in February 2015.

Released under the Official Information Act 1982

## 7. Related Initiatives

### 7.1 Building on existing initiatives

Existing programmes already provide services to high-risk gang individuals and families, or target the criminal offending by gang or transnational crime group members. The whole-of-government action plan on gangs is consistent with and supports existing initiatives but allows for a more specific gang focus. Current work within government portfolios includes the Minister of Justice's paper on a *Stronger Response to Domestic Violence*, the Associate Minister of Social Development's papers on *Family Violence: Achieving Intergenerational Change* and *Government Response to the Report of the Expert Advisory Group on Family Violence*, and the Minister of Corrections' paper on *Progressing the Sentencing (Electronic Monitoring) Amendment Bill*. The action plan on gangs also aligns with the Youth Crime Action Plan, Social Sector Trials and the All-of-Government Response to Organised Crime.

A particular focus of the wider social sector is on reducing family violence. Many women connected with gangs also have significant alcohol and drug or mental health issues that need to be treated at the same time as family violence if lasting change is to be achieved. There are also particular and unique safety concerns in supporting family violence victims in the gang environment.

Other programmes that work with vulnerable families and communities or target organised crime groups include:

- Whānau Ora,
- the Methamphetamine Action Plan,
- Welfare Fraud Collaborative Programme,
- the Organised and Financial Crime Agency New Zealand,
- the Department of Corrections Approach to Reducing Re-offending by Offenders with Gang Connections,
- National Drug Policy and the Children's Action Plan.

Other multi-agency initiatives that relate to the Gangs Action Plan include:

- Organised Crime and anti-Corruption Legislation Bill (Ministry of Justice lead)
- Deported offenders: reciprocal information exchange arrangement to be established and development of a register (MoJ lead)
- Law Commission report on the use of security sensitive information in court proceedings
- National Cyber Security Strategy
- Inter-agency working group on people trafficking.

## Briefing Note

16 February 2016

---

**To** Hon Christopher Finlayson: Minister in Charge of NZSIS; Minister Responsible for GCSB; Attorney-General

**From** Howard Broad, Deputy Chief Executive, Security & Intelligence, DPMC

**For your** Information

**Subject** Joint Five Country Ministerial / Quintet of Attorneys-General: Session 3: Cyber: Encryption s6(a)

---

### Purpose

1. This note briefs you on the s6(a) topic for the cyber session of the upcoming Ministerial. It has been prepared by the National Cyber Policy Office (NCPO).

### Background

2. s6(a) submitted a paper on the challenges for law enforcement agencies of encrypted communications services provided by ISPs s6(a)

s6(a), 6(b)

s6(a), 6(b)

s6(a), 6(b)

Released under the Official Information Act 1982

## Briefing Note

16 February 2016

---

<b>To</b>	Hon Christopher Finlayson: Minister in Charge of NZSIS; Minister Responsible for GCSB; Attorney-General
<b>From</b>	Howard Broad, Deputy Chief Executive, Security & Intelligence, DPMC
<b>For your</b>	Information
<b>Subject</b>	Joint Five Country Ministerial / Quintet of Attorneys-General: Session 3: Cyber: Background Reading: Cyber Security Issues

---

### Purpose

1. This note provides you with additional background material to support your participation in the discussion on cyber security at the upcoming Ministerial. It has been prepared by the National Cyber Policy Office (NCPO).

### Cyber Security Issues

2. There are a range of cyber threats (state-sponsored espionage, cybercrime, politically motivated attacks etc); a range of victims (government agencies, businesses, individuals etc); and a range of involved agencies as well as the private sector.

3. It is a complicated landscape – there are no clean lines or neat boxes between types of threats and victims – and therefore few clean lines exist between the agencies involved in responding to these threats.

4. International best practice (e.g. the OECD) emphasises the importance of a national Strategy and also a central agency to coordinate responses to cyber incidents. We have observed the experience of similar-sized countries – such as the Netherlands, Singapore and Estonia – and engage closely with our Five Eyes partners. There is much to emulate from the way in which these countries are handling cyber security – and also opportunities to New Zealand to nimbly leap ahead – using our size to advantage and ensuring we make the most from the digital economy.

5. Communications Minister Amy Adams launched a refreshed **New Zealand Cyber Security Strategy** in Auckland on 10 December, at a business-focused launch event with senior representatives from across the New Zealand business community, including major ICT, telecommunications, financial, energy and other sector leaders.

6. The Strategy provides a framework for government action – in partnership with the private sector. It brings coherence to a complicated policy and operational area. It also gives confidence to the private sector, NGOs, and international partners that New Zealand is taking cyber security seriously. It sends a signal about New Zealand's serious intent – including to investors.



7. The Strategy's vision is "**a secure, resilient and prosperous online New Zealand**". The refreshed Strategy is intended to help position cyber security as an issue of economic and societal wellbeing as much as a national security issue. The **four goals** of the Strategy are "Cyber Resilience", "Cyber Capability", "Addressing Cybercrime" and "International Cooperation".

8. The **four principles** underpinning the Strategy are: "partnerships are essential", "economic growth is enabled", "national security is upheld", and "human rights are protected online".

9. The Strategy is premised on partnership with the private and NGO sectors as cyber security is not something that the government can do alone.

10. It's not just a Strategy – there is also an **Action Plan** setting out a multi-layered approach to cyber security. There is no single silver bullet. It emphasises that, while technological defences are effective, strong cyber security requires a multi-layered approach.

11. The Action Plan contains a balanced set of initiatives: some underway, such as the implementation of CORTEX, and many needing greater impetus.

12. The Action Plan will be reviewed annually to ensure the actions are current, to report against progress, and to recommend new actions as these are identified. The Strategy, and Action Plan, will help us measure and direct progress towards New Zealand's cyber maturity.

13. The decision to establish a **national CERT** is a major new initiative. This new body will act as a central reporting mechanism for the full range of cyber incidents in New Zealand, and will be the internationally-recognised point of contact where cross-border cooperation is required to manage an incident. This will bring New Zealand into line with our partner countries, most of which have already established CERTs. The details of the CERT, including its legal form, will be considered by Cabinet in the first half of 2016, through the Budget process.

14. Currently, there are gaps in New Zealand's response to cyber security incidents, particularly for small-to-medium enterprises and in responding to cybercrime. It is not clear where New Zealanders and businesses should go for help and authoritative advice. New Zealand's response to cyber incidents could be better coordinated. The establishment of a CERT will help to address these issues.

15. We would like to thank our partners for their advice in the course of developing the Strategy – particularly in the work on developing a national CERT.

16. We'll be continuing to work on developing the new initiatives over the next few months and would value partner assistance, particularly on the CERT and developing a cyber credentials scheme.

# SUMMARY OF NEW ZEALAND'S Cyber Security Strategy:

A secure, resilient and prosperous online New Zealand

New Zealand is increasingly reliant on information communication technology and an open, trusted Internet. Internet connectivity is an integral part of New Zealand's economic growth and international competitiveness.

But this technology provides opportunities for those with criminal or hostile intentions. The 2015 Cyber Security Strategy signals the government's commitment to ensuring New Zealand is safe, resilient and prosperous online.

New Zealand's scale and relatively simple telecommunications and network structure enables the public and private sector to work closely together to embed a cyber security culture, and to respond nimbly to evolving cyber risks.

## WHAT IS CYBERSPACE?

The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.

## Cyber Security Goals

FOUR INTERSECTING GOALS WILL CREATE A  
SECURE, RESILIENT AND PROSPEROUS ONLINE NEW ZEALAND:

### CYBER RESILIENCE

New Zealand's information infrastructures can resist cyber threats and we have the tools to protect our national interests



### CYBER CAPABILITY

New Zealanders, businesses and government agencies understand cyber threats and have the capability to protect themselves

## NEW ZEALAND'S Cyber Security Strategy

### ADDRESSING CYBERCRIME

New Zealand improves its ability to prevent, investigate and respond to cybercrime



### INTERNATIONAL COOPERATION

New Zealand protects and advances its interests on cyberspace issues internationally

# Principles underpinning the Cyber Security Strategy

## PARTNERSHIPS ARE ESSENTIAL

The government has a role to play in cyber security – but not on its own. Close partnerships with the private sector and non-government organisations are required. Businesses drive the New Zealand economy and depend on the Internet and networked technology. They must protect the information that is critical to their commercial success. The private sector owns and operates the telecommunications systems. The private sector and technical community also have considerable cyber security expertise.

The Connect Smart partnership is a public-private collaboration focused on driving cyber security improvement in New Zealand. Connect Smart includes a growing network of banks, telecommunication companies, ICT companies, software companies, social media, retail organisations, education institutions, non-government organisations, community groups, sectoral bodies, business associations and government agencies.

## ECONOMIC GROWTH IS ENABLED

Strong cyber security practices will result in businesses remaining productive, profitable and transparent to customers and shareholders. New Zealand will be recognised as a desirable place to do business, store data, innovate and invest.

ICT and enhanced connectivity will continue to boost economic growth, and the costs of cyber insecurity will be minimised.

## NATIONAL SECURITY IS UPHELD

Cyber threats to New Zealand – particularly state-sponsored espionage, cyber terrorism, theft of intellectual property from government and critical national infrastructure – are national security risks. Upholding New Zealand's national security in the face of this threat is a fundamental principle of this Strategy.

## HUMAN RIGHTS ARE PROTECTED ONLINE

The openness of the Internet is part of its unique value – allowing for unrestricted participation and the free flow of information.

Cyberspace should be a trusted medium, where users have confidence in the integrity of information and the protection of their private and financial details. They should be able to engage online without suffering harm or unlawful interference.

Human rights apply online as they do offline. This includes the right to freedom of expression, and the protection of privacy, as set out in New Zealand law and existing international law.

## Cyber Security Strategy Action Plan

The Cyber Security Strategy is accompanied by a living Action Plan. This Plan will evolve to keep pace with technology developments and the emergence of new threats. New actions may be added, and existing actions amended.

The National Cyber Policy Office will work with government agencies and Connect Smart public-private cyber security partners to produce a public annual report on progress.

### CYBER RESILIENCE



- Set up a national CERT<sup>1</sup>
- Vigorously protect New Zealand's most important information infrastructures
- Use cyber tools to further New Zealand's national security interests
- Prepare for major cyber incidents

### CYBER CAPABILITY



- Expand Connect Smart activities and partnership
- Improve the cyber security capability of small and medium enterprises
- Boost the cyber security capability of the corporate sector, including national infrastructure, and the public sector
- Promote cyber security education and training, including building a cyber security professional workforce
- Support cyber security research and business innovation

### ADDRESSING CYBERCRIME



- Build capability to address cybercrime
- Adapt New Zealand's policy and legislative settings for the digital age
- Enhance New Zealand's operational response to cybercrime
- Use New Zealand's international connections to fight cybercrime

### INTERNATIONAL COOPERATION



- Promote internet governance and norms of state behaviour that reflect New Zealand's interests
- Build networks of international operational cooperation
- Contribute to international cyber security capability and confidence
- Maximise the economic opportunities of cyberspace for New Zealand and New Zealanders

<sup>1</sup> CERT was once an acronym for 'computer emergency response team'. Since 1997, CERT has been a registered trademark owned by Carnegie Mellon University and is no longer used as an acronym. New Zealand is requesting permission to use the CERT trademark.

## Briefing Note

16 February 2016

**To** Hon Christopher Finlayson: Minister in Charge of NZSIS; Minister Responsible for GCSB; Attorney-General

**From** Howard Broad, Deputy Chief Executive, Security & Intelligence, DPMC

**For your** Information

**Subject** Joint Five Country Ministerial / Quintet of Attorneys-General: Session 4: Foreign Investment in Critical Infrastructure: Presentation and Discussion of Foreign Investment Working Group Recommendations

### Purpose

1. This item reports some real progress of the Critical Five (C5) Foreign Investment Working Group, in response to directions received from Five Country Ministers in 2015. Work is ongoing, and the scope of work is widening.

### Background

2. The Working Group has focused on identifying and addressing vulnerabilities that can result from foreign ownership of critical infrastructure, which is of increasing concern amongst New Zealand's Five Eyes partners. The Working Group has begun facilitating information sharing, discussion of and collaboration on broader foreign investment trends, challenges and approaches.

3. s6(a)
- 4.
- 5.


6. s9(2)(g)(i) DPMC officials are developing a policy

**RESTRICTED**

position which reflects of New Zealand's national interests. We expect to bring you an outline position in April 2016.

7. Traditionally, the C5 lens has been on critical infrastructure, and Treasury has focused on the resilience of critical infrastructure. However, like our partners, New Zealand is exposed to wider risks and issues from foreign ownership of critical infrastructure and economic assets.
8. The effect of aggregate foreign investment, particularly for foreign investment risk assessment processes, has been identified as the key issue for future work. The impact of aggregate foreign investment is highly relevant to New Zealand, given our small economy, reliance on a few key primary export sectors, open investment posture, and (to date) lack of consideration of classified material in inward investment policy and decision making.

9. s6(a), 6(b)



**RESTRICTED**



IN-CONFIDENCE

DEPARTMENT  
of the PRIME MINISTER  
and CABINET



## BRIEFING: Five Country Ministerial 2017 – Briefing materials available to date

Date:	21 June 2017	Tracking number:	1617/NSP/008
Security classification:	In confidence	Priority:	Routine
For:	Noting	Required by:	N/A

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
John Beaglehole	Director, National Security Policy	(04) 817 8558	s9(2)(a)	✓
Sara Dib	Senior Policy Advisor, National Security Policy	(04) 819 8247	s9(2)(a)	

Minister's office to complete:

☒ Approved☐ Declined☐ Noted☐ Needs change☐ Seen☐ Overtaken by Events☐ See Minister's Notes☐ Withdrawn

Comments:



Hon Christopher Finlayson  
Minister Responsible for the GCSB  
Minister in Charge of the NZSIS

## BRIEFING: Five Country Ministerial 2017 – Briefing materials available to date

Date:	21 June 2017	Tracking number:	1617/NSP/008
Security classification:	In confidence	Priority:	Routine
For:	Noting	Required by:	N/A

### Purpose

This briefing attaches the briefing materials available to date for the Five Country Ministerial in Ottawa on June 26 2017, for noting. We welcome any comments you may have at this stage. We are still confirming briefings for two agenda items with the Ministry of Business, Innovation and Employment, which is leading those briefings. We are hoping to confirm those materials shortly and will provide the complete bound materials to your office tomorrow (Thursday 22 June 2017).

### Recommendations

The Department of the Prime Minister and Cabinet recommends that you:

1. **note** the attached materials to date for the Five Country Ministerial, which is taking place on 26 June 2017 in Ottawa;
2. **note** that briefings for two agenda items are still being confirmed with the Ministry of Business, Innovation and Employment; and
3. **note** that a complete bound copy of all materials will be provided to your office on Thursday 22 June 2017.

John Beaglehole  
Director, National Security Policy  
Department of the Prime Minister and Cabinet  
Date:

Hon Christopher Finlayson  
Minister Responsible for the GCSB  
Minister in Charge of the NZSIS  
Date:



## Update

1. Attached to this briefing are the briefing materials available to date for the Five Country Ministerial, which is taking place on 26 June 2017 in Ottawa. The Quintet of Attorneys-General takes place the next day.
2. We are still confirming the briefing materials for two agenda items with the Ministry of Business, Innovation and Employment (MBIE), which is responsible for leading the preparation of those items. These agenda items relate mainly to MBIE's areas of responsibility. We are hoping to confirm these briefings shortly. We have therefore added placeholders in the attached materials.
3. We will provide complete bound copies to your office tomorrow (Thursday 22 June 2017). The bound materials will include the agenda, papers for each agenda item, and our briefing materials. We will also provide these materials to Minister Woodhouse's office, as he is also attending the Five Country Ministerial.
4. GCSB has also prepared some separate briefing papers on the Telecommunications (Interception Capability and Security Act 2013) and Project CORTEX, should you wish to provide partners with further information. We will include copies of those briefings with the final materials.
5. Out of scope



Released under the Official Information Act 1982

FIVE COUNTRY  
**MINISTERIAL**



# Five Country Ministerial

Monday 26 June 2017 | Ottawa, Canada

Materials and briefing papers

Released under the Official Information Act 1982

## Index

<b>1</b>	Agenda Seating arrangements
<b>2</b>	Session 1: Intelligence briefing / Counterterrorism
<b>3</b>	Session 2: Countering Violent Extremism <ul style="list-style-type: none"><li>- Briefing note</li><li>- Paper and attachments</li></ul>
<b>4</b>	Session 3: Refugees, migration and screening <ul style="list-style-type: none"><li>- Briefing note</li><li>- Paper and attachments</li></ul>
<b>5</b>	Lunchtime session: National security transparency <ul style="list-style-type: none"><li>- Briefing note</li><li>- Paper</li></ul>
<b>6</b>	Session 4: Security cooperation and law enforcement <ul style="list-style-type: none"><li>- Briefing note</li><li>- Paper and attachments</li></ul>
<b>7</b>	Session 5: Cyber security and encryption <ul style="list-style-type: none"><li>- Briefing note</li><li>- Paper and attachments</li><li>- s6(a)</li><li>- Additional background material provided by GCSB</li></ul>
<b>8</b>	Contact details for New Zealand delegation

# FIVE COUNTRY MINISTERIAL



## FCM 2017 & FCM/Quintet Joint meeting: Detailed Schedule

TIMING		MINISTERS ARRIVAL : June 25
All day		<i>Bilateral Meetings (Fairmont Château Laurier)</i>
		CONFERENCE DAY 1: June 26 (CSIS HQ, Ottawa)
		FCM Plenary
8:00 – 9:30	SESSION 1: Intelligence Briefing / Counterterrorism	s6(a)
	s6(a)	
9:30 – 10:45	SESSION 2: Countering Violent Extremism	s6(a)
	s6(a)	
10:45-11:00	Health break	
11:00 – 12:00	SESSION 3: Refugees & Migration	s6(a)
	s6(a)	
12:15 – 13:30	FCM Lunch	
	- Served lunch for Ministers and Attorneys General in Director Boardroom	
	Discussion on Transparency/Accountability	s6(a)
	- Buffet-style lunch for other members of delegation in Lounge area	
		FCM/QUINTET JOINT MEETING
13:45-15:00	SESSION 4: Security Cooperation & Law Enforcement	s6(a)
	s6(a)	




# FIVE COUNTRY MINISTERIAL



15:00 – 15:15	<i>Health break – Family Photo</i>
15:15 – 16:30	<b>SESSION 5: Cyber Security &amp; Encryption</b> s6(a) s6(a)
16:30 – 17:00	<b>Conclusion</b> <ul style="list-style-type: none"> <li>- <b>Communique Agreement (ALL)</b></li> <li>- <b>Closing Remarks (CAN)</b></li> </ul>
17:00 – 19:00	<i>Bilateral Meetings (CSIS HQ or Fairmont)</i>
19:30 – 22:00	<b>Reception and Dinner (Sir John A. Macdonald Building)</b> <i>Speakers: (TBC)</i>
<b>TIMING</b>	<b>CONFERENCE DAY 2: June 27 (Fairmont Chateau Laurier Hotel)</b>
8:30 – 12:00	<i>Bilateral Meetings</i> <i>(Fairmont Château Laurier)</i>
9:00 – 17:00	<b>Quintet Plenary</b> <i>(see Quintet Draft Agenda)</i>

Released under the Official Information Act 1982

**Session 1: Intelligence briefing / counter terrorism**

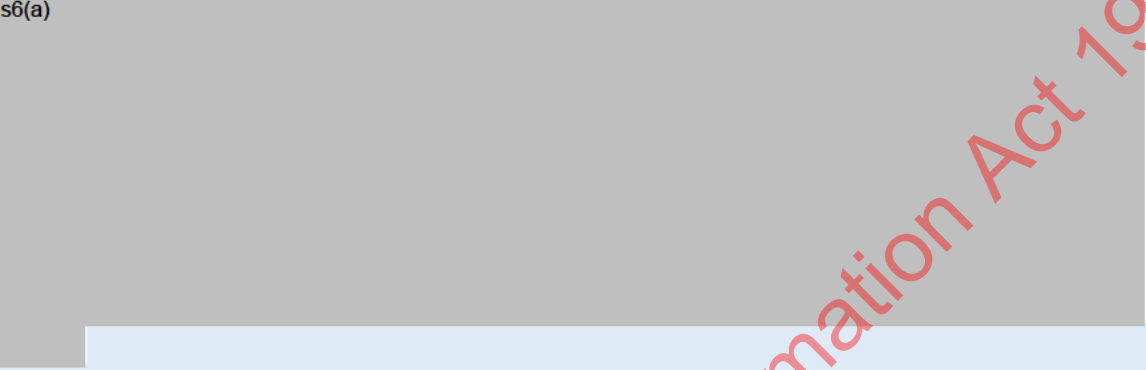

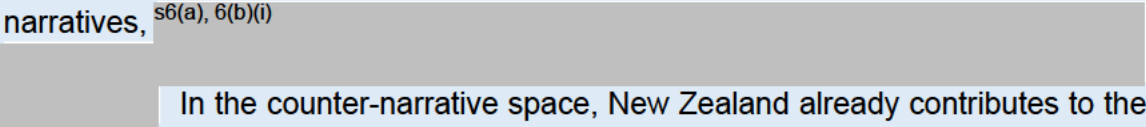
1. <sup>s6(a), 6(b)(i)</sup>
- 

2. There are no papers for this agenda item.

Released under the Official Information Act 1982

## Session 2: Countering Violent Extremism (CVE)

### Talking points

- New Zealand supports members jointly endorsing the industry-led forum on tackling terrorist use of the internet. I also support us sending a joint letter of support for those measures, as proposed by s6(a) (see agenda item 5 for a copy of the letter).
- s6(a)  

- Following the recent London terror attacks, there has been quite a lot of discussion around working with partners to reach international agreements that regulate cyberspace to prevent terrorism. We would advocate caution in this area. Any action to take a treaty-based approach would be a shift away from the current norms-based approach to governing state behaviour in cyberspace.
- s6(a)  

- Our international cyber security policy is premised on an open, innovative and secure cyberspace and on respect for human rights online. We - like other member countries - are committed to supporting internet freedoms and protecting fundamental human rights online. Our CVE measures need to be consistent with those measures.
- We support ongoing joint engagement with the communication service providers (CSPs) to build relationships that allow us to seek assistance with decryption and terrorist content online where possible. Collective engagement by Five Eyes governments is more likely to result in action to support our objectives.
- We also support the other measures proposed by s6(a) to counter radicalisation, such as building digital resilience, discussing the efficacy and impact of counter-narratives, s6(a), 6(b)(i)  


In the counter-narrative space, New Zealand already contributes to the work of the Global Coalition against Daesh in its counter narrative/communications work (one of the Coalition's five lines of effort).



- Regrettably, there is not a great deal of research in this area, and so it is not clear what works and why. The proposed measures will support us to counter and manage radicalisation online.

- s6(a), 6(b)(i)

- We also support s6(a) proposals in respect of returning foreign terrorist fighters, which include promoting comprehensive approaches to managing fighters, sharing best practice, and developing a compendium of our approaches to rehabilitation options. New Zealand faces a much smaller problem than other member countries in this respect, but we all would benefit from shared approaches and understanding.

3. The Five Country Ministerial will discuss joint efforts to counter the spread of violent extremism and recruitment efforts by extremist groups promoting ideological positions that advocate violence to achieve their objectives.

4. The meeting will focus on two priority areas in the draft action plan prepared by the Countering Violent Extremism Working Group:

- s6(a), 6(b)(i)


5. The challenge we face in terms of violent extremism and terrorist content is of a different nature and magnitude to our partners. s6(a), 6(b)(i)

6. Regrettably, there is not a great deal of research in this area, and so it is not clear what works and why; from New Zealand's point of view, developing a stronger understanding of indicators of radicalisation to violence is as valuable as some of the other work underway.

7. Fundamentally, New Zealand's approach to preventing violent extremism focuses on building strong and engaged communities that do not allow radical and extremist views to flourish. We can do so because of the far smaller number of individuals and communities of concern in New Zealand, owing in part to New Zealand looking to

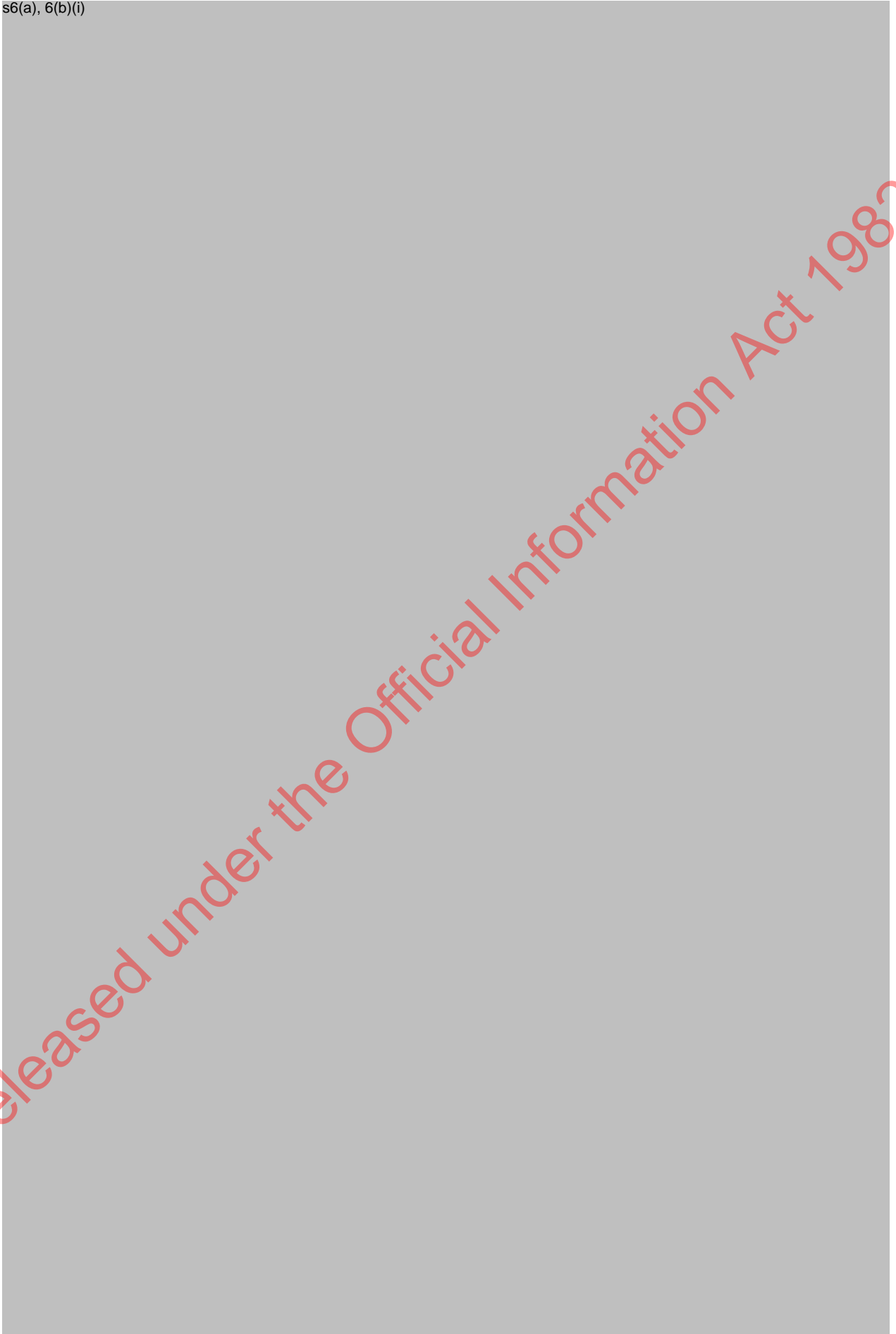
integrate new communities. Different migration patterns have aided this – we have largely taken immigrants from communities that integrate well, although this has changed in the last decade or so, with the result that our communities are increasingly diverse (for instance, 39% of the Auckland population was born overseas). Nonetheless, officials remain focused on ensuring that new New Zealanders do not feel themselves to be the victims of discrimination.

s6(a), 6(b)(i)




Released under the Official Information Act 1982

s6(a), 6(b)(i)



Released under the Official Information Act 1982

s6(a), 6(b)(i)



Released under the Official Information Act 1982

### Session 3: Refugees and migration

#### Talking points

s6(a), 6(b)(i)

- New Zealand already offers eGate (branded as SmartGate in Australia and New Zealand) to the Migration 5 nationalities. This functionality will be extended, probably in July, to the arrival and departure of eChip passport holders from China. This will be followed shortly after by eChip passport holders from Germany, France, the Netherlands, Sweden, Norway, Singapore and Austria.
- New Zealand is working hard on developing better and less intrusive border processing mechanisms for travellers. Along with Australia, we also have a strong ongoing interest in maintaining high biosecurity screening standards, and this is a key principle in our border strategy development.


s6(a), 6(b)(i)

s6(a), 6(b)(i)

~~IN CONFIDENCE~~

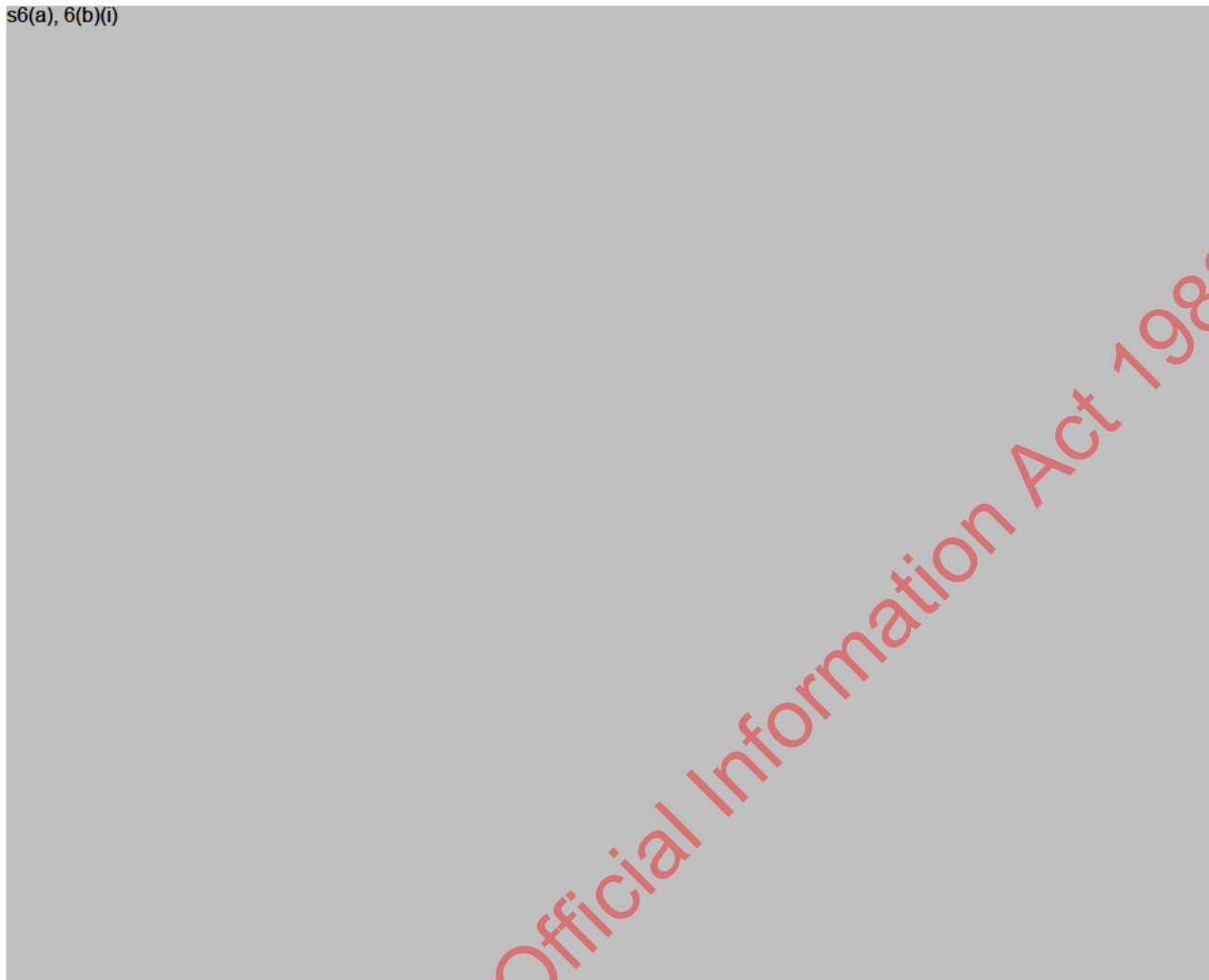
Five Country Ministerial 2017  
26 June 2017 Ottawa

s6(a), 6(b)(i)




Released under the Official Information Act 1982

s6(a), 6(b)(i)



s6(a), 6(b)(i)



13. New Zealand is actively engaged in exploring opportunities to use technology better to manage border risks. The border agencies (which in New Zealand also include the Ministry of Primary Industries, because of the importance of good biosecurity management to our economy) are currently developing a refreshed Border Strategy.
14. New Zealand's Border Strategy is strongly focused on economic outcomes and gains, rather than simply focusing on protection from harm. The importance of ongoing improvements to the customer experience is also emphasised: within the context of an agreed level of risk, the border system should provide users with as efficient, cost-effective, and non-intrusive ("light-touch") service as possible.
15. The working assumption is that the border system will over time move to intervening only where required, with risk assessments done out of sight of customers and not requiring their direct participation. Improvements in technology and more integrated risk assessment will be key to achieving this.
16. In the immediate future, New Zealand will be offering SmartGate access (arrival and departure) to Chinese holders of eChip passports within a month. This will soon extend

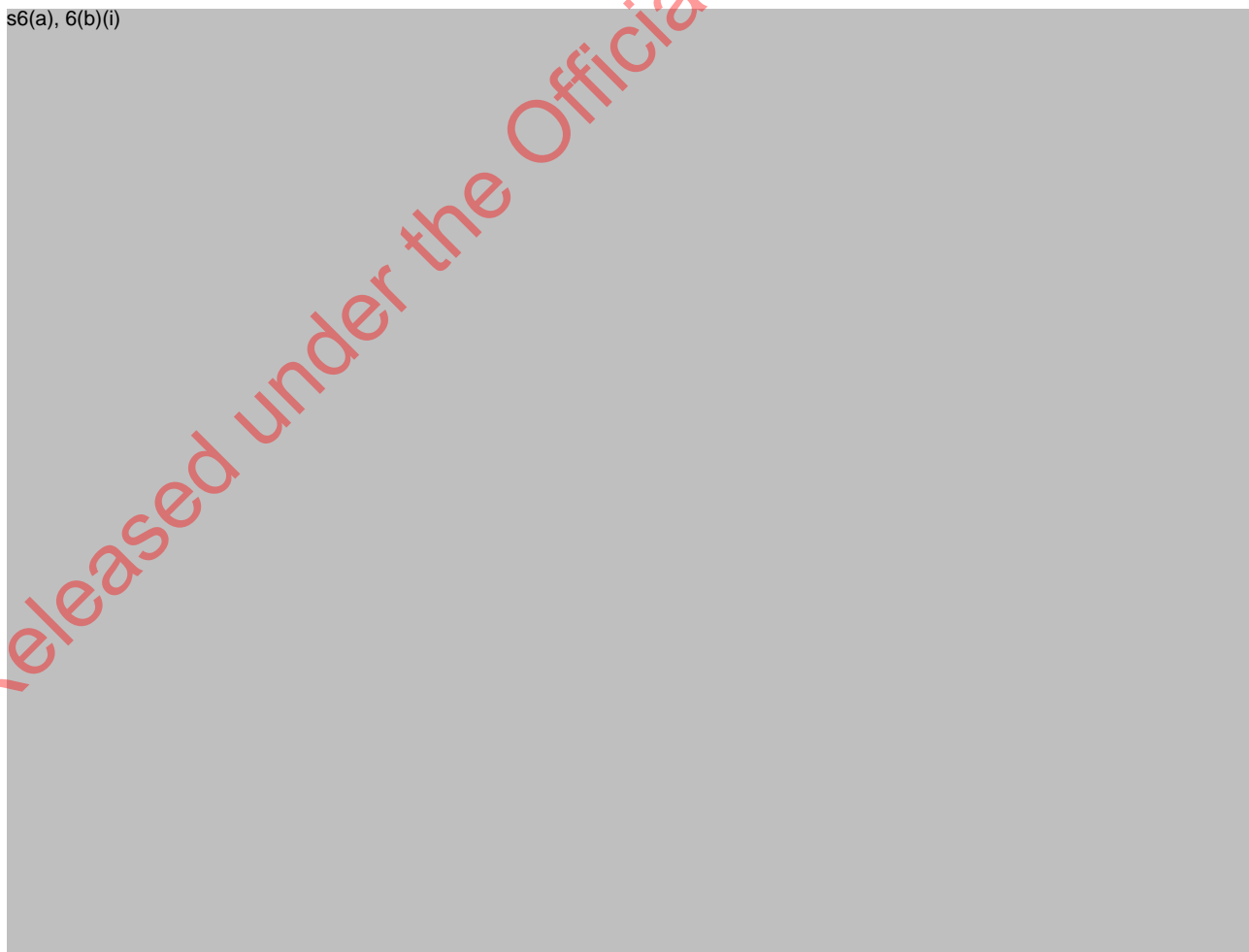


(based on volumes and passport suitability) to a further group of countries (Germany, France, the Netherlands, Sweden, Norway, Singapore and Austria), with further countries expected to be brought in SmartGate functionality before Christmas.

s6(a)

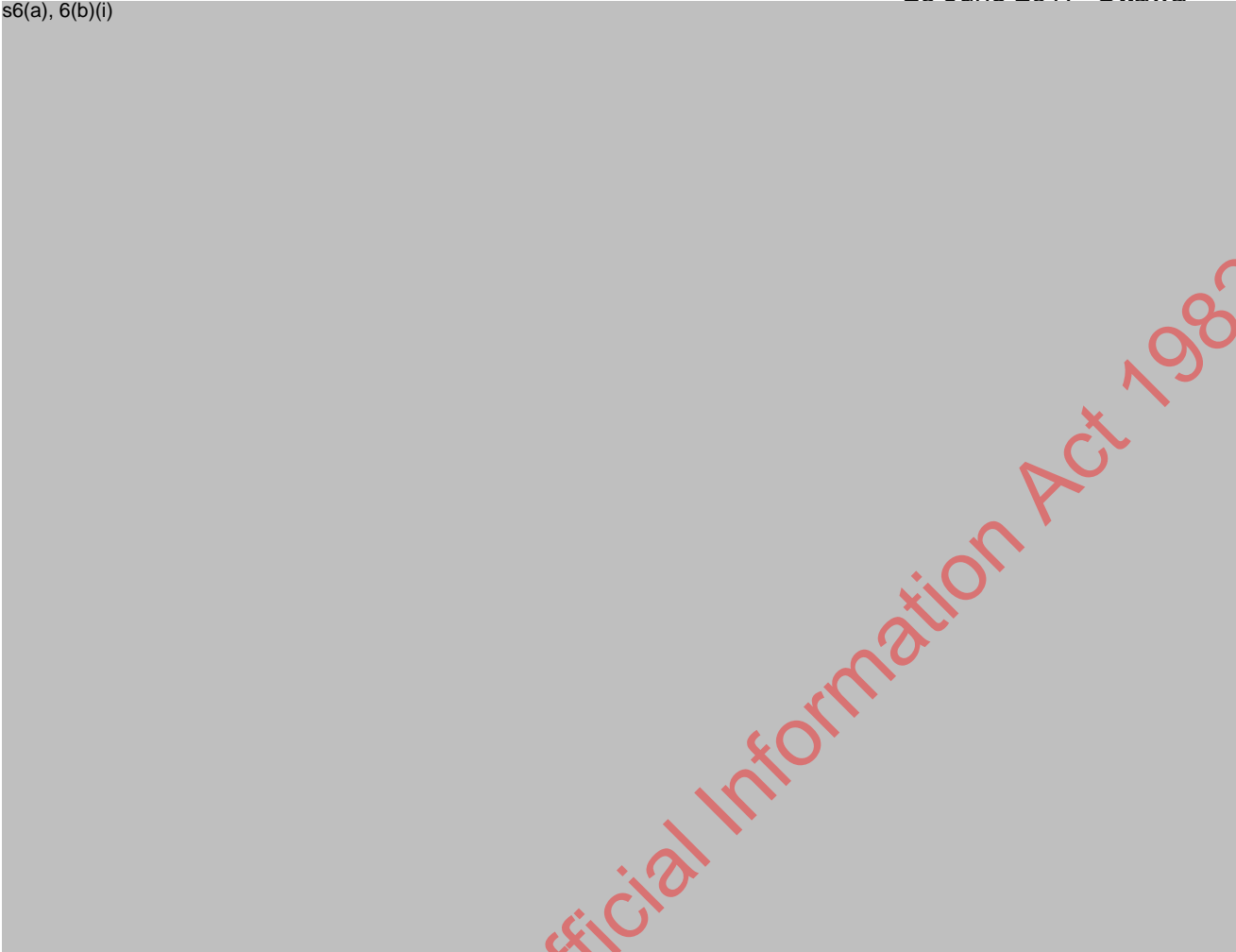


s6(a), 6(b)(i)



Released under the Official Information Act 1982

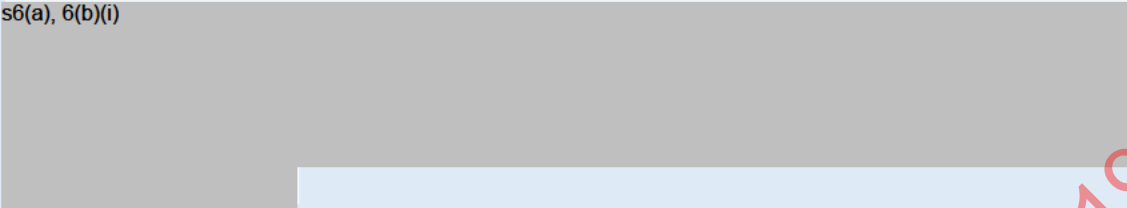
s6(a), 6(b)(i)



Released under the Official Information Act 1982

## Lunchtime session: National security transparency

### Talking points

- s6(a), 6(b)(i)  

- Most of these principles are already reflected in our existing arrangements. For example:
  - The legislation governing the intelligence and security agencies and their oversight bodies was recently reformed. Instead of four Acts, we now have one (the Intelligence and Security Act 2017). The Act makes it clearer and easier for members of the public to understand what the GCSB and NZSIS do. It also strengthened the oversight applying to these agencies, improving transparency and accountability.
  - New Zealand agencies – including the intelligence and security agencies – are subject to the Privacy Act 1993. That Act sets out 12 information privacy principles that govern how personal information is to be collected, used, stored and disclosed. The Intelligence and Security Act 2017 significantly increased the number of information privacy principles applying to the intelligence and security agencies.
  - The new Act also makes it a criminal offence for people holding a security clearance, or people who have been given access to classified information on a confidential basis, to wrongfully communicate, retain or copy classified information. This will help to protect classified information.
  - As a counterpart, the Act clarifies who government employees (other than GCSB or NZSIS staff) can make protected disclosures involving classified information to (those staff must currently must make disclosures to the Ombudsman, rather than the Inspector-General of Intelligence and Security).
- We welcome discussion at the FCM about measures that could be taken to further implement the transparency principles.
- We note that the Canadian government has recently tabled a Bill that would create a new oversight body for the Canadian intelligence and security agencies. In New Zealand changes have been made to strengthen the intelligence and security agencies' oversight bodies (for example, funding for the office of the Inspector-General of Intelligence and Security was significantly increased and changes were made to her legislative regime to remove perceived barriers to her independence and to increase the scope of what she can enquire into). Those moves were well-

received by the public and reflect a strong desire for accountability and transparency.

## Proposals

1. The Five Country Ministerial will be asked to agree to a number of transparency principles and will discuss potential next steps to implement the principles within relevant agencies.

s6(a), 6(b)(i)

## Comment

3. Most of these principles are already reflected in our existing arrangements. For example:

3.1. The legislation governing the intelligence and security agencies and their oversight bodies was recently reformed. Instead of four Acts, we now have one (the Intelligence and Security Act 2017). The Act clearly lays out the intelligence and security agencies' powers, making it clearer and easier for members of the public to understand what the GCSB and NZSIS do. It also strengthened the oversight applying to these agencies, improving transparency and accountability.

3.2. New Zealand agencies – including the intelligence and security agencies – are subject to the Privacy Act 1993. The Act sets out 12 information privacy principles that govern how personal information is to be collected, used, stored and

disclosed. The Intelligence and Security Act 2017 significantly increased the number of information privacy principles applying to the intelligence and security agencies.

- 3.3. The new Act also makes it a criminal offence for people holding a security clearance, or people who have been given access to classified information on a confidential basis, to wrongfully communicate, retain or copy classified information. This will help to protect classified information. As a counterpart, the Act clarifies who government employees (other than GCSB or NZSIS staff) can make protected disclosures involving classified information to (those staff must currently must make disclosures to the Ombudsman, rather than the Inspector-General of Intelligence and Security).
4. There may be a case for New Zealand to take further measures to improve citizens' understanding of national security activities and to engage citizens to better understand the national security threat environment and possible policy responses.
5. One of the aims of the *First Independent Review of Intelligence and Security in New Zealand* (which led to the new legislation) was to build public trust and confidence in the intelligence and security agencies. While the legislation and supporting factsheets goes some way towards that, better engagement by the agencies (and the government more broadly) with the public about their activities and the threat environment would support this. Both Directors of the agencies have taken pro-active steps in this area, which is to be welcomed.

**Session 4: Security cooperation and law enforcement**

s6(a), 6(b)(i)

Released under the Official Information Act 1982

s6(a), 6(b)(i)


Released under the Official Information Act 1982



s6(a), 6(b)(i)


Released under the Official Information Act 1982

s6(a), 6(b)(i)



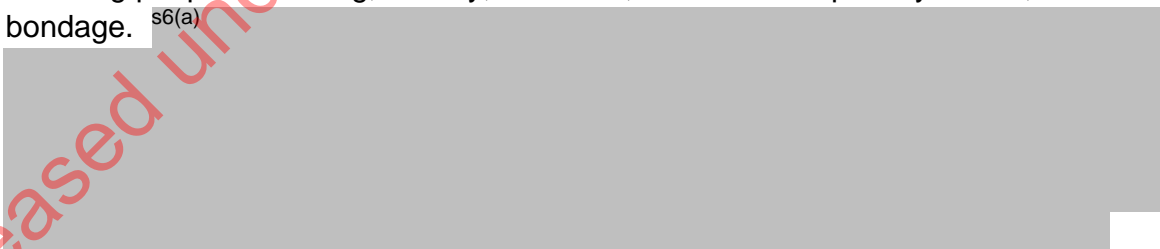
**To improve our collective ability to attack modern slavery and disrupt known human traffickers**

17. s6(a), 6(b)(i)



New Zealand's focus, however, will continue to be through the *Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime*.

18. Modern slavery is an umbrella term used to describe a range of exploitative practices, including people trafficking, slavery, servitude, forced or compulsory labour, and debt bondage. s6(a)



19. s6(a)



*New Zealand's main focus is through the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime*

20. New Zealand's main focus for combating modern slavery and human trafficking is through the *Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime*. A major new initiative is the Bali Process Government and Business Forum, which will bring together ministers and business leaders from the region to harness the combined efforts of government and the private sector to combat human trafficking, slavery and forced labour.
21. The Forum will be driven by the private sector, with participants guiding the discussion and developing their own program of work. Rob Fyfe, Chairman of Ice Breaker, is New Zealand's business representative. The agenda is likely to focus on issues such as labour recruitment practices; supply chain transparency; remediation mechanisms; and legal mechanisms that have a positive impact on company behaviour.
22. The Forum will take place in Perth on 24-25 August 2017 and will be co-chaired by Hon Julie Bishop MP, Minister for Foreign Affairs of Australia and H.E. Ms Retno Marsudi, Minister for Foreign Affairs of Indonesia.

**We support the suggested communiqué line**

s6(a)



## FCM/Quintet Joint Session

### Session 5: Cyber Security & Encryption

#### Paper A: Encryption s6(a), 6(b)(i)

##### Talking points

- s6(a), 6(b)(i)
- We acknowledge that there is no simple solution to the challenge posed by encryption, as strong encryption is a fundamental element of good cyber security.  
s6(a)
- Under section 24 of New Zealand's Telecommunications (Intercept Capability and Security Act) 2013 (TICSA) both network operators and service providers have a duty to assist in the execution of interception warrants and other lawful interception authorities issued to the Police or an intelligence and security agency. This duty includes decrypting communications where the network operator or service provider has provided the encryption
- s6(a)
- s9(2)(g)(i)
- We welcome the opportunity to discuss ways to address this challenge, including by building stronger relationships with Communications Service Providers (CSPs).
- s6(a), 6(b)(i)
- [REDACTED]

- Encryption and cyber-security risks are not issues that governments can solve alone. We will need to work closely with the CSPs to develop workable solutions s9(2)(g)(i)

- s6(a), 6(b)(i)

- s9(2)(g)(i)

1. This session will focus on the challenges ubiquitous encryption is creating for law enforcement and national security agencies, including some recent examples, s6(a), 6(b)(i)

## Background

2. The proliferation of communications that offer end-to-end encryption is allowing criminals and terrorist groups to secure their communications against lawful acquisition by law enforcement or national security agencies. s6(a)

3. Currently, there is no good solution to the challenges posed by encryption. The trade-off is not one between privacy and security but one between more security and less security. Strong encryption is a fundamental element of good cyber security, which is increasingly critical to New Zealand's national security and economic prosperity. Many common online activities (eg, banking) rely on strong encryption. Any attempt to build a 'back-door' into an encrypted system creates a vulnerability that could be exploited by a range of actors.

## New Zealand's legislative settings

4. Under section 24 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) both network operators and service providers have a duty to assist in the execution of interception warrants and other lawful interception authorities issued to the Police or an intelligence and security agency. This duty includes decrypting communications where the network operator or service provider has provided the encryption (s24(3)(vi) of TICSA).

5. The obligation in TICSAs is useful but it is limited to any encryption that the network operator or service provider assisting under the warrant has themselves placed on communications. <sup>s6(a)</sup>

[REDACTED]

6. <sup>s9(2)(g)(i)</sup>

[REDACTED]

7. <sup>s9(2)(g)(i)</sup>

[REDACTED] Providers may also refuse to provide information in order to protect their brand or the privacy of their customers <sup>s9(2)(g)(i)</sup>


8. <sup>s9(2)(g)(i)</sup>

[REDACTED]

<sup>s6(a), 6(b)(i)</sup>

[REDACTED]

s6(a), 6(b)(i)



Released under the Official Information Act 1982



**Paper B: Cyber security / Response to Critical Cyber Incident**

**Talking points**

- s6(a), 6(b)(i)
- 
- In responding to WannaCry, CERT NZ engaged with a number of international CERTs – including Five Eyes partners - to determine the extent of the ransomware attack, the mechanism for infection and possible solutions.
- We see great value in Five Eyes collaboration s6(a)
- Four areas of activity under New Zealand's *Cyber Security Strategy* were prioritised in 2016:
  - setting up a national CERT (CERT NZ became operational in April 2017)
  - developing a cyber credentials scheme to provide cyber security solutions for small businesses in New Zealand
  - closing the skills gap and building a cyber professional workforce by developing new cyber security qualifications, and
  - addressing cybercrime, including progressing work to accede to the Council of Europe Convention on Cybercrime as part of a Law Commission review of search and surveillance legislation.
- Additional areas of work include the consideration of security issues related to the Internet of Things (IoT) and the development of an innovation plan to grow New Zealand's own cyber security industry, including through lifting research and development and addressing skills and workforce constraints.
- s6(a), 6(b)(i)

s6(a), 6(b)(i)

- 

### **Introduction to project CORTEX – talking points provided by GCSB**

- The number and nature of cyber threats in New Zealand continues to grow in line with international trends - threatening our economy and potentially undermining our strategic advantage.
- CORTEX is a project to implement a suite of capabilities that counter cyber threats to organisations of national significance in New Zealand.
- This include government departments and private sector organisations such as key economic generators, niche exporters, research institutions, and operators of critical national infrastructure.
- These capabilities are operated by the GCSB's National Cyber Security Centre (NCSC).
- All of the capabilities operate with the explicit consent of the organisations in scope for them.
- CORTEX has a particular focus on countering foreign-sourced malware that is particularly advanced in terms of technical sophistication and/or persistence. Malware of this type is not adequately mitigated by commercially available tools.
- The CORTEX capabilities allow malicious software (malware) to be passively detected as well as actively disrupted.
- CORTEX includes the pilot of a malware disruption capability called "Malware-Free Networks".

- s6(a)

- The CORTEX project is nearing its end, and moving into an initial operating capability.

- s6(a), 6(b)(i)

- s6(a), 6(b)(i)

1. This item highlights the ongoing value in close Five Eyes collaboration on cyber security. It provides Ministers with an overview of the key Five Eyes cyber groups, an update on recent developments and suggests areas for further cooperation. The paper does not seek direction from Ministers but is instead an opportunity to brief Ministers on the workstreams already underway in officials' groups.

### Operational incident response

2. s6(a), 6(b)(i)

3.

4.

5.

6. The WannaCry ransomware has been reported as the most significant ransomware campaign seen in history. It was assessed as a "medium-severity" event in terms of New Zealand's Cyber Security Emergency Response Plan (CSERP), meaning no formal national security mechanisms were activated – WannaCry's impact in New

Zealand was fortunately very limited. CERT NZ was the lead agency coordinating New Zealand's response, working closely with the NCSC in the GCSB and the National Cyber Policy Office (NCPO) in the Department of the Prime Minister and Cabinet (DPMC). s6(a), 6(b)(i)

### Strategic cyber-security policy issues

7. s6(a), 6(b)(i)
- 8.
- 9.

### New Zealand's Cyber Security Strategy and Action Plan (2015)


10. Four areas of the Strategy were prioritised in 2016:

- setting up a national CERT (action 1 of the resilience goal)
- developing a cyber credentials scheme for small business (action 2 of the capability goal)
- closing the skills gap and building a cyber professional workforce (action 4 of the capability goal), and
- addressing cybercrime (the third goal of the Strategy).

11. Good progress has been made in the first three of these priority areas and a number of other key areas of the Action Plan as set out below. These developments mean that New Zealand's cyber security capacity is increasingly mature – something that has been recognised by our Five Eyes partners. But there is more to be done to fulfil the ambitious and comprehensive Action Plan.


12. **CERT NZ** has been operational since April 2017. As a central part of New Zealand's cyber security architecture, CERT NZ will receive reports of cyber incidents, analyse threats, share information and advice, coordinate incident responses and be an international point of contact.
13. A **cyber credentials** package has been tested with a sample of small businesses and is in the process of being scaled-up for the New Zealand small business market. A **Cyber Security Skills Taskforce** has been established and is developing a level 6 cyber security diploma for delivery in polytechnics.
14. **Cyber Resilience:** The delivery of Project CORTEX malware detection and disruption services by the NCSC to a select group of organisations of national importance is on track. Provision has been made in the Defence White Paper for improved cyber protection of New Zealand Defence Force networks and operations. New Zealand's readiness to handle a significant cyber incident is being tested through exercises in accordance with the Cyber Security Emergency Response Plan.
15. **Cyber Capability:** New Zealand's first Cyber Security Summit was held in May 2016. It emphasised the importance of cyber security to the executive and governance levels of the New Zealand economy. The 2016 Connect Smart campaign focused on cyber security in the workplace. There has been improvement – albeit from a low base – in the privacy and security protection of government information.
16. **Addressing Cybercrime:** There has been less progress in addressing cybercrime, due to competing priorities and limited resources. Work to accede to the Council of Europe Convention on Cybercrime (also known as the Budapest Convention) and resourcing of NZ Police cyber training would improve the capability of NZ Police to deal with cybercrime.

17. s6(a), 6(b)(i)




18. Work is ongoing in all of the above areas. Additional areas include the consideration of security issues related to the Internet of Things (IoT) and the development of an innovation plan to grow New Zealand's own cyber security industry, including through lifting research and development and addressing skills and workforce constraints. Minister Bridges has a keen interest in progressing this work.

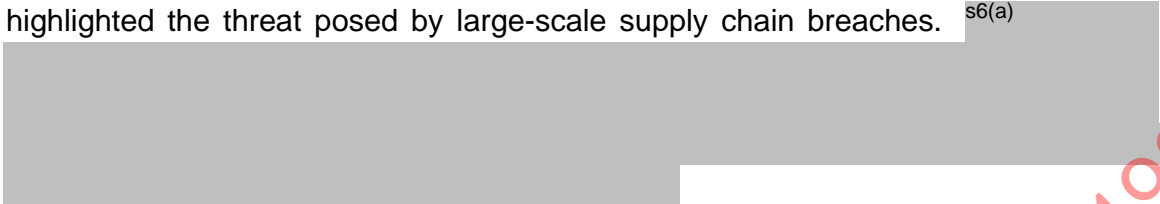
19. s6(a), 6(b)(i)



s6(a), 6(b)(i)

A large rectangular area of the document has been redacted with a solid grey fill.

20. Policy work is also ongoing following the global compromise of MSPs, which highlighted the threat posed by large-scale supply chain breaches. s6(a)

A large rectangular area of the document has been redacted with a solid grey fill.

Released under the Official Information Act 1982





GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI

## Briefing Paper

### Background on the Telecommunications (Interception Capability and Security) Act 2013

**To** Hon. Christopher Finlayson, Minister Responsible for GCSB  
**From** Andrew Hampton, Director GCSB  
**For your** Information  
**Date** 21 June 2017

#### Action sought

		Timeline
<b>Note</b>	The UNCLASSIFIED background on the Telecommunications (Interception Capability and Security) Act 2013	Routine
<b>Consider</b>	Passing a copy of the attached note to your FVEY Attorneys-General colleagues	Routine

#### Contacts for telephone discussion (if required)

Name	Position	Telephone	1 <sup>st</sup> Contact
6(a)	Chief Legal Adviser	9(2)(a)	X

### Background on the Telecommunications (Interception Capability and Security) Act 2013



UNCLASSIFIED

1. This note sets out the policy basis and mechanics of the Telecommunications (Interception Capability and Security) Act 2013 (**TICSA**).
2. It has been prepared at an UNCLASSIFIED level for you to share with your Five Eyes Attorneys-General colleagues.

---

Andrew Hampton  
Director, GCSB

## Recommendations

It is recommended that you:

<b>Note</b>	The UNCLASSIFIED background on the Telecommunications (Interception Capability and Security) Act 2013.	yes / no
<b>Consider</b>	Passing a copy of the attached note to your FVEY Attorneys-General colleagues.	yes / no

---

Hon Christopher Finlayson  
Minister Responsible for the GCSB

June 2017



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI

## Rationale for and mechanics of the Telecommunications (Interception Capability and Security) Act 2013

### Background to and rationale for TICSA

#### Repealing and replacing 2004 legislation

3. TICSA was passed on 11 November 2013, repealing and replacing the Telecommunications (Interception Capability) Act 2004 (**TICA**).
4. The new Act had two main objectives (as set out in the Bill's explanatory note):
  - a. To ensure that interception obligations applying to the telecommunications industry were clear, did not impose unnecessary compliance costs and were sufficiently flexible to respond to current and future operations, needs and technological developments; and
  - b. To require network operators to engage with the Government on network security matters, inform the Government of certain proposed decisions, courses of action, or changes in relation to an area of "specified security interest", and work with the Government to apply any specific risk-based and proportionate security measures.
5. TICSA achieved these by changing the existing interception-related obligations on the telecommunications industry, and introducing a new 'network security' regime with GCSB as the regulator.
6. While both GCSB and NZ Police have statutory roles under TICSA, the Ministry of Business, Innovation and Employment (**MBIE**) was the lead agency for the Bill's development and is now the Act's administering agency. This paper focuses on GCSB's roles under TICSA.

#### Rationale for key aspects of the TICSA

##### Changes to interception capability duties

7. Companies operating New Zealand's public telecommunications networks (network operators) were required to be capable of intercepting telecommunications on their networks and separately to assist surveillance agencies give effect to lawful interception authorities, under the 2004 TICA (the duty to assist also applied to service providers). The two duties are complementary – the interception capability obligation requires companies to 'design-in' the ability to intercept telecommunications (equipment and staff), and the duty to assist requires companies to then use that or other capability to give effect to specific interception authorities.
8. TICSA made a number of changes to the existing interception capability obligations on network operators, including the following.



- a. Reducing the obligations on some (smaller) network operators –the surveillance agencies (GCSB, NZSIS or Police) are less likely to need smaller operators (with fewer customers) to intercept communications and so while these companies are always subject to the duty to assist should a case arise, they do not need to design-in interception capability to their networks from the outset. They do need to be willing to work with interception agencies to enable interception on their networks, however.
  - b. Allowing the Minister to extend interception capability obligations to companies providing telecommunications services to end users in New Zealand (service providers, like Skype) – in many instances it is service providers rather than network operators that hold the communications agencies like GCSB, NZSIS and the Police seek to intercept. Service providers are always subject to the duty to assist give effect to a particular interception authority. This provision allows an additional requirement to be imposed on specific service providers to design-in an interception capability to their service.
9. As noted in MBIE's departmental report on the 2013 TICS Bill, these changes sought to ensure that obligations – and compliance costs – are targeted and tailored to operational needs.

#### Accessing encrypted communications

- 10. TICS Bill did not change the nature or scope of the obligation on network operators to remove any encryption they had placed on communications on their network prior to providing it to agencies.
- 11. TICS Bill did make plain reasonable assistance with decryption (removing encryption the assisting entity had themselves placed on communications) was part of the duty to assist surveillance agencies give effect to an interception authority. TICS Bill also made it clear it was only encryption imposed by the network operator or service provider themselves that had to be lifted, and not encryption applied by a third party.
- 12. The obligation to assist in accessing encrypted communications is set out in greater detail in our separate classified briefing to you, but in summary:
  - a. Network operators (and service providers if deemed in by the Minister) are required to design their interception capability to enable decryption of telecommunications where the network operator is the entity that applied the encryption; and
  - b. When assisting surveillance agencies give effect to an interception authority, and regardless of whether the network operator has any interception capability duty, the duty to decrypt any encrypted intercepted telecommunications where the network operator is the entity that has applied the encryption.
- 13. Submissions on these provisions in the 2013 TICS Bill expressed the concern that they could be interpreted to require network operators to introduce security vulnerabilities, or weaken their encryption. The departmental report stated this is not the case as the obligation is limited to requiring the network operator (and any deemed in service providers) to remove encryption it has itself imposed, it does not weaken the encryption or create security vulnerabilities.



### Offshore companies

14. TICSAs also clarify the position of offshore network operators and service providers. It states the duty to assist surveillance agencies to give effect to an intelligence authority applies regardless of where the company is based, as long as it meets the TICSAs definitions of network operator or service provider.
15. Possible jurisdictional issues arise if a New Zealand surveillance agency sought to give effect to an interception authority by requiring an offshore company operating in New Zealand to act on it. That company may be subject to contradictory laws in its home jurisdiction preventing it providing assistance on the New Zealand authority.
16. On this issue, the Departmental Report reasons as the duty to assist only requires "reasonable assistance" to help fulfil a warrant, conflict with extraterritorial legal obligations would limit what could reasonably be required. This was considered an appropriate case-by-case outcome, which did not involve removing the obligation to assist for all offshore providers.

### Introduction of new network security regime

17. The network security regime established in Part 3 of TICSAs was a new regulatory framework imposed on network operators in 2013.
18. The purpose of Part 3 of TICSAs is to prevent, sufficiently mitigate, or remove 'network security risks'. These are national security risks arising from the design, build, or operation of public telecommunications networks, or from interconnections to or between public telecommunications networks in New Zealand or with networks overseas.
19. The central aspect of the network security regime is the obligation on network operators to notify the Director of the GCSB of any proposed decision, course of action or change regarding areas of specified security interest on their networks. The duty to notify covers decisions about procurement as well as changes to the architecture of a network and changes affecting ownership, control, oversight and supervision of networks.
20. Following notification, the Director assesses whether the proposal raises a network security risk. The assessment requires consideration of both the impact on the network (compromise of the network, impairment of the confidentiality, availability, or integrity of communications on the network) and the potential effect of such an event on the provision of core services (central or local government service, health services etc). Where a risk is identified, the network operator is notified and not able to do further work to implement the change. It is then required to submit a mitigation proposal.
21. If after considering a mitigation proposal, a significant network security risk remains, the Director of the GCSB can refer the matter to the Minister for decision. TICSAs provides for the Director and Minister to consider different factors in making decisions. The Director's assessments are tied to technical security factors, whereas the Minister must also take into account the impact on the network operator or meeting the costs associated with a Ministerial direction, and the potential consequences the direction may have on competition and innovation in telecommunications markets.
22. The timing of notification is central to the operation of the framework. For procurement, notification is required before any steps are taken to approach the



market. Other changes or decisions require notification during the development of a business or change proposal – i.e. before the change is implemented.

23. The intent of this framework is to enable the Government and industry to work collaboratively and co-operatively to identify and address network security risks. Given its expertise in telecommunications and access to classified information about threats to New Zealand's networks, it is appropriate for this regulatory responsibility to sit with GCSB. The Part 3 TICSAs regime formalises an existing practice of collaboration and cooperation between GCSB and network operators on network security risks.
24. The Departmental Report noted that "the Government is concerned to ensure that the design, build and operation of our telecommunications networks do not provide easy access to other entities to allow them to turn off or degrade networks and services, steal intellectually property, alter data or intercept peoples' communications without appropriate authority". While network operators had relationships with various departments, including GCSB, to this end, a formal framework was considered required to ensure, among other things,
  - a. all network operators engage with government (creating a level playing field) and factor in security protections with more complete information;
  - b. Government has formal enforcement rights in the rare cases where they are necessary – given the importance of network security the government cannot simply rely on network operators acting alone to mitigate and understand the risk.

#### ***Notification regarding interception capability equipment***

25. A network operator must also notify the Director of the GCSB under Part 3 of TICSAs before undertaking work to meet its interception capability duties under Part 2. Lawful interception equipment is an area of particular interest given its exploit value to threat actors.

#### **Mechanics of TICSAs**

##### **Compliance and enforcement**

26. TICSAs made changes to the compliance and enforcement framework, seeking to increase compliance with the Act. Those changes included:
  - a. Requiring network operators to register with the Government (NZ Police is the Registrar), providing basic information for the register and advising of changes, including when a network operator moves from one level of interception capability obligations to another.
  - b. Enabling a designated officer (individuals appointed by the Commissioner of Police) to require network operators to provide information for specified purposes, including to support a surveillance agency to enforce compliance with the interception capability duties of TICSAs.
  - c. Requiring network operators to nominate a suitable employee for secret-level government-sponsored security clearance.
27. TICSAs also introduced a graduated enforcement regime enabling minor non-compliance to be dealt with by way of a breach notice, and serious non-compliance dealt with in the High Court.

28. While these formal compliance and enforcement measures are important, GCSB has yet to rely on them to enforce any of the obligations in Parts 2 or 3.

## **Part 2 – Interception capability and duty to assist**

### **Interception capability**

29. TICSAs do not specify how network operators should meet their interception capability duties. Instead, it sets out the things a surveillance agency will be able to do to give effect to an interception authority when the network operator has complied with its duty. As such, other than through the Part 3 network security regime, there is no statutory role for GCSB in respect of network operators interception capability.
30. Network operators can be exempted by a designated officer (appointed by Commissioner of Police) from their interception capability obligations. GCSB has a role in advising on proposed exemptions – TICSAs require that the agency be consulted and the primary consideration for the designated officer is national security or law enforcement interests.

### **Duty to assist**

31. GCSB regularly seeks the assistance of network operators and service providers to give effect to interception authorities – currently interception warrants and access authorisations issued under s 15A of the GCSB Act 2003. GCSB relies on the duty to assist in s 24 of TICSAs to require entities to assist.

## **Part 3 – Network security**

32. The network security provisions of TICSAs came into force in April 2014. GCSB has a Regulatory Unit <sup>s6(a)</sup> providing advice to the Director and delegated decision makers on the assessments required under TICSAs.
33. GCSB engages with the community of network operators through ad-hoc meetings and a yearly 'roadshow' across all major New Zealand cities. Select staff within network operators have obtained SECRET level security clearances to enable GCSB to share sufficient details of network security risks to enable network operators to prepare effective mitigation plans.
34. As of June 2017, GCSB has received 284 notifications under Part 3 TICSAs. The majority of these raised no or a minimal network security risk. Eleven notifications raised a more than minimal or significant network security risk. Following engagement between GCSB and network operators, seven of those eleven notifications were withdrawn, or the identified network security risks prevented or sufficiently mitigated.
35. The remaining four notifications were only recently identified and the network operators are currently developing mitigation proposals.





GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI

## Briefing Paper

### Introduction to project CORTEX

**To** Hon Christopher Finlayson, Minister Responsible for GCSB  
**From** Andrew Hampton, Director, GCSB  
**For your** Information  
**Date** 21 June 2017

### Action sought

		Timeline
<b>Note</b>	The UNCLASSIFIED talking points on Project CORTEX	Routine
<b>Note</b>	The UNCLASSIFIED background on Project CORTEX	Routine
<b>Consider</b>	Passing a copy of the attached note to your FVEY Attorneys-General colleagues	Routine

### Contacts for telephone discussion (if required)

Name	Position	Telephone	1 <sup>st</sup> Contact
6(a)	Deputy Director, IACD	9(2)(a)	X
	Assistant Director		



UNCLASSIFIED

## Introduction to project CORTEX

Please find enclosed an unclassified background on Project CORTEX, for circulation to your counterparts at the upcoming Quintet meeting as you see appropriate. Also enclosed are talking points to support any related discussion.

---

Andrew Hampton  
Director, GCSB

## Recommendations

It is recommended that you:


<b>Note</b>	The UNCLASSIFIED talking points on Project CORTEX	yes / no
<b>Note</b>	The UNCLASSIFIED background on Project CORTEX.	yes / no
<b>Consider</b>	Passing a copy of the attached note to your FVEY Attorneys-General colleagues.	yes / no

---

Hon Christopher Finlayson  
Minister Responsible for the GCSB

\_\_\_\_\_ June 2017

## Introduction to project CORTEX – talking points

1. (U) The number and nature of cyber threats in New Zealand continues to grow in line with international trends - threatening our economy and potentially undermining our strategic advantage.
2. (U) CORTEX is a project to implement a suite of capabilities that counter cyber threats to organisations of national significance in New Zealand.
3. (U) This include governments departments, and private sector organisations such as key economic generators, niche exporters, research institutions, and operators of critical national infrastructure.
4. (U) These capabilities are operated by the GCSB's National Cyber Security Centre (NCSC).
5. (U) All of the capabilities operate with the explicit consent of the organisations in scope for them.
6. (U) CORTEX has a particular focus on countering foreign-sourced malware that is particularly advanced in terms of technical sophistication and/or persistence. Malware of this type is not adequately mitigated by commercially-available tools.
7. (U) The CORTEX capabilities allow malicious communications (malware) to be passively detected as well as actively disrupted.
8. (U) CORTEX includes the pilot of a malware disruption capability called "Malware-Free Networks".
9. s6(a) 
10. (U) The CORTEX project is nearing end, and moving into an initial operating capability.
11. (U) New Zealand has greatly benefitted from partner support to develop this project and we are grateful for this input.
12. (U) As we embed and scale this cyber defensive capability, it increasingly enables us to provide unique information to our security partners and to contribute to international efforts to counter advanced cyber harms.





GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI

## Overview of GCSB CORTEX cyber security initiative June 2017

### Purpose

1. (U) This paper provides an overview of the Government Communications Security Bureau's (GCSB) CORTEX initiative.

### Background

2. (U) CORTEX is a project to implement a suite of capabilities that counter cyber threats to organisations of national significance in New Zealand – e.g. to operators of critical national infrastructure. This includes governments departments, and private sector organisations such as key economic generators, niche exporters, research institutions, and operators of critical national infrastructure.
3. (U) The CORTEX capabilities allow malicious communications (malware) to be passively detected as well as actively disrupted.
4. (U) These capabilities are operated by the GCSB's National Cyber Security Centre (NCSC).
5. (U) All of the capabilities operate with the explicit consent of the organisations in scope for them.
6. (U) Some of the capabilities involve GCSB receiving a copy of the internet communications of the organisations directly benefitting from the malware detection. Some also involve a role for internet service providers (ISPs) and in one case (see "Malware-Free Networks Pilot", below) – ISPs share the lead on this.
7. (U) Aspects of CORTEX are highly classified. However, a great deal of information about the initiative has been put in the public domain via the GCSB's website ([www.gcsb.govt.nz/our-work/information-assurance/#cortex](http://www.gcsb.govt.nz/our-work/information-assurance/#cortex)).
8. (U) Delivery of CORTEX is an important – and explicit – part of the New Zealand Cyber Security Strategy.

### CORTEX operation

9. (U) CORTEX operates with the explicit agreement of the organisations that it protects.
10. (U) CORTEX operates under the GCSB Act, 2013, with the legal authority transferring to the Intelligence and Security Act, 2017 when this act comes into effect in September.
11. (U) The detection and disruption of malware by GCSB is currently governed by warrants and access authorisations approved by the Minister Responsible for GCSB and the Commissioner of Security Warrants.
12. (U) CORTEX has a particular focus on countering foreign-sourced malware that is particularly advanced in terms of technical sophistication and/or persistence. Malware of this type is not adequately mitigated by commercially-available tools.
13. (U) The protections delivered by CORTEX are important because malicious cyber activity can cause significant harm in terms of:

## UNCLASSIFIED

- theft of intellectual property (e.g. of unique research, technical designs, or commercially-sensitive business proposals)
  - loss of customer data (such as credit card details)
  - destruction or unauthorised dissemination of private communications
  - holding of data for "ransom" (wherein data is made inaccessible until a ransom is paid)
  - damage to IT networks or disruption to services relying on them.
14. (U) Malicious cyber activity affects individual public and private sector organisations and has implications for New Zealand's economy and security.

### Malware-Free Networks Pilot

15. (U) CORTEX includes the pilot of a malware disruption capability called "Malware-Free Networks".
16. (U) Malware-Free Networks espouses the principle that the active disruption of malware is best undertaken by ISPs and therefore potentially at significant scale.

17<sup>s6(a)</sup>



### CORTEX implementation

18. (U) The implementation phase of the CORTEX initiative is nearing completion and the capabilities are delivering the level or result envisaged in the project business case.
19. (U) CORTEX is helping prevent harm to New Zealand's significant organisations that would not otherwise be detected or mitigated.
20. (U) Through its operation, we are able to provide unique information to our security partners and to contribute to international efforts to counter advanced cyber harms.

### NZ threat environment and recent operational activity

21. (U) The number and nature of cyber threats in New Zealand continues to grow in line with international trends - threatening our economy and potentially undermining our strategic advantage.
22. (U) We have a voluntary reporting regime and the threats recorded here are just those reported to us or detected by our own capabilities.
23. (U) Our NCSC recorded 338 incidents during the 2015/16 financial year, 148 more than in the 2014/215 period.
24. (U) This increase is primarily due to the expanding capacity of the NCSC to detect and respond to more incidents. We believe this trend - driven by increased capacity - will continue in the current financial year.
25. (U) Of the 338 incidents recorded in 2015/16, 169 were associated with public sector entities and at least 73 involved the private sector; the remainder involved individuals, small businesses and some instances where we were unable to identify the victim
26. (U) The types of incidents detected and disrupted by CORTEX include:
- The stealing of credentials - personal details and system log on information - after users were tricked into entering their details into a fake website



**UNCLASSIFIED**

Foreign, likely state- supported, actors attempting to gaining access to multiple networks

- Sustained - brute force - attempts to gain access to a network holding valuable intellectual property, and
- The insertion of malicious code into a legitimate website in an attempt to gain access to that user's network.

27. (U) If allowed to achieve their objective these intrusions could result in substantial harm to important networks and the loss or manipulation of information important for the operation or future prosperity of New Zealand.

28. (U) These types of threat are not unique to the kinds of organisations protected by our CORTEX capabilities. All New Zealand organisations are vulnerable to the broad range of cyber threats.

Released under the Official Information Act 1982

UNCLASSIFIED

## CORTEX FAQs (from GCSB website)

### What is CORTEX?

CORTEX is a project to counter cyber threats to organisations of national significance – e.g. to operators of critical national infrastructure.

CORTEX involves GCSB implementing capabilities to protect these organisations against advanced malicious software ('malware'). The capabilities will allow advanced malware to be detected and disrupted.

CORTEX operates with the explicit agreement of the organisations that are protected from cyber threats.

CORTEX operates under the GCSB Act. The detection and disruption of malware by GCSB is governed by warrants and access authorisations approved by the Minister Responsible for GCSB and the Commissioner of Security Warrants.

Background to the project is seen in redacted Cabinet papers available on the [beehive.govt.nz](http://beehive.govt.nz) website.

### What is the purpose of CORTEX?

CORTEX's only purpose is to counter cyber threats to organisations of national significance.

CORTEX has a particular focus on countering foreign-sourced malware that is particularly advanced in terms of technical sophistication and/or persistence. Malware of this type is not adequately mitigated by commercially-available tools.

Countering cyber threats helps to protect New Zealand's economy and security. CORTEX therefore contributes to implementation of New Zealand's Cyber Security Strategy. Information about New Zealand's Cyber Security Strategy is available at [dpmc.govt.nz](http://dpmc.govt.nz) (external link) and [connectsmart.govt.nz](http://connectsmart.govt.nz).

The protections delivered by CORTEX are important because malicious cyber activity can cause significant harm in terms of:

- theft of intellectual property (e.g. of unique research, technical designs, or commercially-sensitive business proposals)
- loss of customer data (such as credit card details)
- destruction or unauthorised dissemination of private communications
- holding of data for "ransom" (wherein data is made inaccessible until a ransom is paid)
- damage to IT networks or disruption to services relying on them.

Malicious cyber activity affects individual public and private sector organisations and has implications for New Zealand's economy and security.

A number of organisations are involved in improving New Zealand's cyber security. These include NetSafe, the NZ Internet Task Force, the National Cyber Policy Office (part of the Department of the Prime Minister and Cabinet), the New Zealand Police, the New Zealand Security Intelligence Service, the Department of Internal Affairs, and the Connect Smart partnership.

UNCLASSIFIED



## UNCLASSIFIED

### Which organisations receive the CORTEX protections?

Some are public sector organisations and some are businesses. The organisations include government departments, key economic generators, niche exporters, research institutions, and operators of critical national infrastructure.

All have been assessed as being of national significance according to criteria determined independently of GCSB.

GCSB does not disclose the identity of the individual organisations receiving the CORTEX protections. Doing so might help to confirm where some of New Zealand's most valuable information is held and so increase the targeting of cyber attacks.

### How is it decided which organisations will be offered the CORTEX protections?

An organisation is offered the CORTEX protections only if it is of national significance – in particular, only if it owns or operates what is termed an 'information asset of national interest' (ANI). A list of such organisations is maintained by the National Cyber Policy Office, which is part of the Department of the Prime Minister and Cabinet (DPMC).

For capacity reasons, CORTEX's scope cannot encompass all organisations on the DPMC list. So government officials oversee a process by which potential CORTEX organisations are selected from it. They consider:

- where each organisation sits on the prioritised DPMC list
- coverage of different sectors
- evidence that a particular organisation, or particular sector, has or is likely to be targeted by advanced malware

### How does CORTEX comply with the law?

One of GCSB's functions relates to information assurance and cyber security. Section 8A of the GCSB Act sets out this function. It is in this capacity that GCSB is implementing CORTEX.

GCSB's access to and use of communications under CORTEX is governed by interception warrants and access authorisations issued jointly by the Minister Responsible for GCSB and the Commissioner of Security Warrants.

### Are ISPs involved in CORTEX?

Yes:

Some ISPs will receive the CORTEX protections directly – e.g. because they operate critical national infrastructure. Where this is the case, the ISP must first agree to receive the protections. The cyber protections will operate in respect of the ISP's corporate communications and information systems (i.e. not those of the ISP's customers). Any benefit to the ISP's customers would be indirect – e.g. because the ISP's corporate network is more resilient to cyber attack.

Some ISPs will be involved in assisting GCSB to provide the protections to other organisations. Where this is the case, the other organisations must be aware of the additional protections and agree to receive them. The situation must be one in which the

## UNCLASSIFIED

**UNCLASSIFIED**

organisation receiving the cyber protections has consented to receiving them by signing a formal deed with GCSB and is aware that an ISP might assist GCSB in providing the protections.

GCSB is currently piloting an initiative called 'Malware-Free Networks' where it will share cyber threat information with an ISP (Vodafone) so that the ISP can actively mitigate malware for a small subset of its customers. Under this arrangement: the benefiting ISP's customers must agree to receive the protections; the customers will be aware of GCSB's support to the ISP; and GCSB does not receive the internet traffic of the participating ISP or any of its customers.

**Are ISPs compelled to be involved in CORTEX?**

No, when this is a question about an ISP receiving the CORTEX cyber protections itself. If an ISP is receiving the protections, this is because the ISP has agreed to this and has signed a deed with GCSB – there is no requirement to do so under law.

No, when this is a question about the planned pilot of the 'Malware-Free Networks' initiative. As part of the pilot GCSB will share cyber threat information with an ISP so that it can mitigate advanced malware that is targeting the ISP's customers. The ISP must agree to participate in the pilot and it must obtain agreement from the small subset of its customers that will receive the cyber protections.

The situation is different, however, when a nationally significant organisation has a signed a deed with GCSB to receive the CORTEX protections and an ISP is assisting GCSB to deliver the protections to that organisation. In this situation:

- the ISP provides the assistance where there is a warrant or authorisation issued by the Minister Responsible for GCSB and the Commissioner of Security Warrants
- the Minister and Commissioner have assessed that the activity described in the warrant or authorisation – including the involvement of the ISP – meets the standards set out in the GCSB Act, including that the activity is justified by the outcome sought
- the ISP has a statutory duty to assist GCSB to give effect to a warrant or authorisation. This means that, when GCSB presents the relevant signed warrant or authorisation to the ISP, the ISP has to assist GCSB.

**How do the protected organisations benefit from the CORTEX capabilities?**

Because of CORTEX, GCSB is able to:

- detect cyber threats to information systems owned or operated by protected organisations
- provide targeted advice on the prevention and mitigation of these threats to those organisations and others
- identify vulnerabilities in computer systems and networks that advanced threats might exploit
- mitigate advanced malware directly.

**UNCLASSIFIED**

UNCLASSIFIED

**Under CORTEX, are cyber threats blocked?**

Yes, in some cases. Some organisations will receive CORTEX protections that provide 'active defence' of their networks or computer systems.

Such active defence involves putting in place systems that can identify and stop cyber threats in real-time. These systems are given 'fingerprints' – patterns of data that identify particular threats – for them to use to distinguish between benign and malicious internet traffic. When malicious internet traffic is identified by a fingerprint, the system prevents it from reaching its destination.

**Does CORTEX involve GCSB looking for spam?**

In most cases, no. However, sometimes email that might be regarded as spam represents a first step to installing malicious software on a victim's computer. GCSB would look to identify and defend against spam of this type for protected organisations of national significance.

ISPs already use technical means to block malicious internet traffic that their customers would otherwise receive. CORTEX's primary focus is malware that takes a particularly severe form and is advanced in terms of technical sophistication and/or persistence. Such malware is less common than spam.

**Does CORTEX require consent?**

Yes. The cyber protections delivered by CORTEX are provided to a limited group of nationally significant organisations who consent to receiving them.

There is no compulsion. The organisations agree to receive the protection only if they see value in doing so.

Consent is confirmed in a formal deed between GCSB and each organisation. The deed sets out the conditions under which GCSB will provide one or more cyber security services to the organisation.

Under the Malware-Free Networks initiative (see below), GCSB will assist an ISP to mitigate malware that is targeting its customers. In this case the agreement will be between the ISP and its customers. The ISP's customers will be aware of GCSB's role in sharing cyber threat information with the ISP. GCSB will not receive any of the internet traffic of the ISP or its customers.

**Does CORTEX involve GCSB analysing the data of consenting organisations?**

In some cases yes – so that cyber intrusions detectable in the data can be identified and advisories can be issued.

Each protected organisation must explicitly agree to this and confirm they have the authority to allow GCSB to access relevant data.

When organisations sign up to receiving CORTEX protection they agree to informing their staff – and, where relevant, others who might interact with their IT systems – that their communications might be accessed for cyber security purposes.

UNCLASSIFIED



**UNCLASSIFIED**

Responsibility for the notification lies with the protected organisation. The notifications are put in place in different ways depending on the nature of the organisation and which of its IT systems receive the CORTEX protections.

The notifications will not name GCSB, as doing so might confirm to potential hackers that particularly sensitive information is processed by the organisation's computer networks.

**Is CORTEX 'cover' for other purposes?**

No. CORTEX's scope is limited to mitigating cyber-borne threats to nationally significant organisations. There is no other reason for the project. The capabilities delivered by CORTEX cannot be used for purposes other than cyber security.

GCSB is not allowed to share CORTEX-derived communications with other government agencies or with any other organisation (domestic or overseas), except in the context of countering cyber threats.

Moreover, if communications of a protected organisation are to be provided to another government agency for cyber security purposes, then the protected organisation must explicitly agree to this.

**Does CORTEX involve 'mass surveillance'?**

No. CORTEX is consented, authorised and highly targeted. The cyber protections are made available to a limited group of public and private sector organisations of national significance – e.g. government agencies, critical infrastructure providers, key economic generators.

The detection and disruption of malware by GCSB is governed by warrants and access authorisations approved by the Minister Responsible for GCSB and the Commissioner of Security Warrants.

These warrants and authorisations do not allow GCSB analysts to have access to the communications of the protected organisations as a matter of course. There is a two-step process whereby GCSB analysts are granted access to relevant data only if a risk has been identified to a particular organisation, and only if the need for the access has been justified to the satisfaction of the Minister Responsible for GCSB and the Commissioner of Security Warrants.

CORTEX does not involve mass or bulk scanning of New Zealand internet (or other) communications. Detection of cyber threats operates in respect of a highly targeted (and consented and authorised) range of communications.

If all eligible organisations signed up to the protections, less than 1% of New Zealand's internet traffic could be involved in CORTEX. Current experience suggests that only a very small proportion of that traffic (0.5% of the 1%) would ultimately be found to contain indications of malicious cyber activity and an even smaller proportion (0.01% of the 0.5%) would need to be looked at by a GCSB analyst, and only following automatic machine-based alerting.

**UNCLASSIFIED**

UNCLASSIFIED

#### **How does automatic machine-based alerting work? Who programs the machines?**

Machine analysis involves computers looking in data for patterns (or 'fingerprints') of known evidence of malicious cyber activity.

These fingerprints tell the computers what to look for and are produced in various ways, often by inspecting a sample of malicious software to understand how it operates and what evidence it leaves behind during a cyber intrusion.

Malicious software samples may be collected after a successful or attempted cyber intrusion has been identified, and the resulting fingerprints can be used to prevent future attacks of the same type, or at least identify when they have happened.

GCSB engineers program the machines. In the same way that GCSB analysts are prohibited from looking at CORTEX data unless it is strictly for the purpose of identifying and defending against malicious cyber activity, GCSB engineers are also prohibited from programming the machines for any other purpose.

#### **Could CORTEX mean a GCSB analyst is reading my email?**

Only in truly exceptional circumstances. All of the following would have to be true:

- you are in email communication with a public or private sector organisation of national significance. Only this email communication could be accessed – your other communications (e.g. to your friends and family, or to other organisations) could not be analysed under CORTEX.
- that organisation has agreed to receiving the CORTEX protections and has advised staff and other (including external) users of its computer systems that the organisation's internet traffic is scanned for cyber security purposes.
- your email correspondence with that organisation of national significance is somehow associated with – e.g. inadvertently carries – malicious cyber activity that machine scanning has flagged as of concern.
- because of a specific risk to the organisation in question, GCSB has been granted a warrant or access authorisation that explicitly allows GCSB analysts to access communications of this type. CORTEX warrants and access authorisations do not allow this access automatically – justification specific to each organisation and a defined period of time is required, with approval given by both the Minister Responsible for GCSB and the Commissioner of Security Warrants.

Even with all these conditions met, all a GCSB analyst would be looking for in an email is evidence of malicious cyber activity. If any such evidence is found, this information could only be used for cyber security purposes.

#### **What is stopping a GCSB analyst from using CORTEX data for the wrong reasons?**

There are multiple checks, both through independent audit and in elements built into systems being used, to ensure information is accessed only for appropriate, authorised purposes.

Access to data is restricted to GCSB staff specifically approved to carry out the analysis. A very limited number of GCSB analysts and engineers have access to CORTEX data. Senior

UNCLASSIFIED



## UNCLASSIFIED

GCSB managers are responsible for overseeing restrictions on access, which is approved for specialists in computer network defence only.

Searches of CORTEX data must be documented by the relevant GCSB analyst before it is undertaken. Any non-compliant use – deliberate or otherwise – would be visible on audit.

Analytical tools supporting CORTEX automatically audit and restrict use of data by GCSB analysts according to the permission under which the data is received.

Machines eliminate the vast majority of data that CORTEX processes as 'not for human analysis' on the basis that the machines cannot find indicators of malicious cyber activity.

In addition, all CORTEX data is categorised according to how it should be handled, making the rules about what can and cannot be done with particular data clear to GCSB analysts. It would be very difficult for someone to accidentally open something they were not meant to open.

The GCSB analysts and engineers hold the highest level of government security clearance. This involves thorough inquisition vetting, including background checks, investigations and interviews.

A GCSB analyst who intentionally looked at something in CORTEX data for their own purposes, knowing that it was not relevant to the provision of cyber protections, would be acting outside of GCSB's legal authority. Like any serious misconduct, this action would be treated very seriously by GCSB and could lead to the analyst losing their job.

GCSB has an internal compliance team that conducts audits of these processes to ensure that GCSB staff are adhering to: the GCSB Act; GCSB policy requirements; and deeds with the individual organisations receiving the CORTEX protections. The internal compliance team checks that rules regarding who can handle the data and what they can do with it are adhered to.

The Inspector-General of Intelligence and Security provides external oversight to ensure that GCSB – including through CORTEX – operates within the law and with propriety, and its compliance systems are sound, and that complaints against GCSB can be independently investigated.

### What are the privacy implications of CORTEX?

A detailed answer to this question is set out in a formal Privacy Impact Assessment (PIA) that has been prepared for CORTEX. A redacted version of the PIA [PDF, 628 KB] is available for download.

### What CORTEX data is shared with GCSB's 5-EYES partners?

The only CORTEX data shared with other 5-EYES cryptologic agencies relates to malicious cyber activity – e.g. what types of cyber attack have been detected in New Zealand.

Like GCSB, these other agencies – ASD, CSE, GCHQ and NSA – have a cyber security mandate. GCSB works with these agencies – and also with the international CERT community – because many cyber threats to New Zealand have an overseas source.

CORTEX does not involve GCSB sharing private New Zealand communications with overseas agencies – e.g. 5-EYES, CERT, security, military, law enforcement or other.

## UNCLASSIFIED



UNCLASSIFIED

Moreover:

- the capabilities delivered by CORTEX cannot be used for purposes other than cyber security
- warrants and access authorisations prevent GCSB from sharing CORTEX-derived data with other government agencies or with any other organisation (domestic or overseas), except in the context of countering cyber threats
- if sensitive communications of a protected organisation are to be provided to another government agency for cyber security purposes, then the protected organisation must explicitly agree to this.

UNCLASSIFIED

Released under the Official Information Act 1982

~~IN CONFIDENCE~~

**Five Country Ministerial/Quintet Conference**  
26 & 27 June 2017 - Ottawa, Canada

DEPARTMENT  
of the PRIME MINISTER  
and CABINET



*New Zealand Delegations' Contact Details*

Name	Contact Number	Email Address
Hon. Christopher Finlayson	9(2)(a)	Christopher.Finlayson@parliament.govt.nz
Hon. Michael Woodhouse		Michael.Woodhouse@parliament.govt.nz
John Beaglehole		9(2)(a) @dpmc.govt.nz
Nigel Bickle		9(2)(a) @mbie.govt.nz
Una Jagose		9(2)(a) @crownlaw.govt.nz
Brendan Horsley		9(2)(a) @crownlaw.govt.nz
Alison Marris		9(2)(a) @parliament.govt.nz
9(2)(a)		9(2)(a) @parliament.govt.nz

1.	Agenda – Five Country Ministerial
2.	Ministerial Priority Statement
3.	Threat Assessments: s6(a), s6(b)(i) [REDACTED]
4.	Cyber current threats and response - Briefing and position paper
5.	5G - Briefing and position paper - s6(a) [REDACTED]
6.	Internet of things and trusted marketplaces - Briefing and position paper - Statement of Intent regarding the Security of the Internet of Things
7.	Drones - Briefing and position paper
8.	Asylum systems abuse and fraud - Briefing and position paper
9.	Data Sharing - Briefing and position paper
10.	Social integration, Inclusion, and Identity - Briefing and position paper
11.	Industry roundtable on child sexual exploitation - Briefing and position paper - Biographies of industry attendees - Background notes s6(a) [REDACTED]
12.	Countering Foreign Interference - Briefing and position paper
13.	Combatting Online Child Exploitation - Briefing and position paper
14.	Countering and Preventing Terrorism and Violent Extremism - Briefing and position paper
15.	Online Safety and Encryption - Briefing and position paper
16.	Foreign Terrorist Fighters and Battlefield Evidence - Briefing and position paper

Out of scope

[REDACTED]

# FIVE COUNTRY MINISTERIAL



Emerging Threats  
London 2019

## AGENDA

29-30 July 2019

### DAY 1

Time	Item	Lead
0815 - 0830	<b>Welcome and Administration</b> <i>Home Secretary welcome, and theme introduction</i>	UK
0830 - 0915	<b>Ministerial statements on priorities</b> <i>Home Secretary to invite other Ministers to introduce short 'priority statements'</i>	ALL
0915 - 1000	<b>Threat Assessments</b> s6(a), s6(b)(i)	s6(a)
1000 - 1015	<b>MORNING TEA</b>	
1015 - 1230	<b>Cyber Threats</b> <i>Current threats and response, inc. NCSC threat assessment</i> <i>Cyber and 5G</i> <i>Session outcomes</i>	s6(a)
1230 - 1330	<b>LUNCH (Ministers +1)</b>	
1330 - 1515	<b>Emerging Technologies</b> <i>'Internet of Things'</i> <i>Drones</i> <i>Session outcomes</i>	s6(a)
1515 - 1530	<b>AFTERNOON TEA</b>	
1530 - 1700	<b>Borders &amp; Immigration</b> <i>Asylum systems abuse &amp; fraud</i> <i>Data sharing</i> <i>Session outcomes</i>	s6(a)
1700 - 1830	<b>BILATERALS</b>	
1830 - 1900	<b>TRANSFER</b>	
1900	<b>DRINKS RECEPTION (All) at White Tower, Tower of London</b>	
2000	<b>DINNER (Ministers +2) in Medieval Palace followed by Ceremony of the Keys</b> <b>Ministerial Discussion: Social integration</b>	
2000 - 2100	<b>DINNER (Other delegates) at White Tower, Tower of London</b>	

FIVE COUNTRY  
MINISTERIAL



Emerging Threats  
London 2019

**AGENDA**

29-30 July 2019

**DAY 2**

Time	Item	Lead
0900 - 1100	<b>Industry Roundtable on CSEA</b> <i>Attended by Microsoft, Twitter, Facebook, Google, Snap &amp; Roblox</i>	ALL
1100 - 1115	<b>MORNING TEA</b>	
1115 - 1200	<b>Countering Foreign Interference</b> <i>Election security and strengthening democracy</i> <i>Session outcomes</i>	s6(a)
1200 - 1230	<b>Draft FCM Communiqué</b>	ALL
1230 - 1315	<b>JOINT FCM/QUINTET LUNCH (Ministers + 1)</b>	

# FIVE COUNTRY MINISTERIAL



Emerging Threats  
London 2019

## AGENDA

29-30 July 2019

### JOINT FCM/QUINTET SESSIONS

Time	Item	Lead
<b>1315 – 1500</b>	<b>Online Harms</b> <i>Countering child sexual exploitation and abuse</i> <i>Preventing terrorist use of the internet and countering extremism</i> <i>Session outcomes</i>	s6(a)
<b>1500 - 1515</b>	<b>AFTERNOON TEA</b>	
<b>1515 - 1615</b>	<b>Encryption</b> <i>Session outcomes</i>	s6(a)
<b>1615 - 1715</b>	<b>Foreign Terrorist Fighters</b> <i>Battlefield evidence, international justice mechanism and PNR/UNSCR 2396</i> <i>Session outcomes</i>	s6(a)
<b>1715 - 1730</b>	<b>Finalise Joint Communiqué</b>	ALL
<b>1730 - 1800</b>	<b>BREAK / BILATERALS</b>	
<b>1800 - 1845</b>	<b>OFFICIAL PHOTOGRAPHS &amp; PRESS CONFERENCE (All Ministers)</b>	
<b>1900</b>	<b>JOINT FCM/QUINTET DRINKS RECEPTION (All) at Gray's Inn</b>	



## **Minister Little – Ministerial Statement of Priorities**

Duration: 650 words, approx. 5 minutes.

### **Opening**

Tēnā koutou, tēnā koutou, tēnā tatou koutou.

Thank you to Secretary Patel, for hosting us in London this morning. I acknowledge this is very early in your tenure as Home Secretary, and thank you for continuing with this meeting. I hope you find the next two days a warm welcome to our ranks.

As you will all be aware, we were originally supposed to be meeting in Manchester, an appropriate place for us to gather given the significance of the events of 22 May 2017<sup>1</sup>. I would therefore first like to acknowledge the 22 victims of the immediate attack, and those who continue to suffer as a result.

New Zealand has always stood firmly alongside its partners in the face of these events. Now we are able to do so with the kind of empathy only direct experience of such an event can bring.

On 15 March 2019, an armed extremist entered two mosques in the city of Christchurch, killing 51 people and injuring many more.

The alleged offender is a right-wing extremist, radicalised in part due to content readily available online.

He also used the internet to gain a worldwide audience for his heinous activity. For New Zealand, this makes our discussions with you on the role of the internet – both the benefits it offers, but also the dangers of unrestricted access – even more pressing.

Since that time, New Zealand has worked with partners from governments worldwide and with digital industry, towards eliminating terrorist and violent extremist content online, through the Christchurch Call to Action. Prime Minister Ardern has dedicated significant energy to addressing this issue, and I am delighted that we will have the opportunity tomorrow to discuss how we can take this work forward.

### **New Zealand's national security priorities**

New Zealand's national security priorities reflect the reality that we are a small, open, and diverse country situated at the very bottom of the world. Our interests are best realised by working with our partners, by following a rules-based international order, and by utilising our strengths as a tolerant nation with a proud Pacifica history.

---

<sup>1</sup> On 22 May 2017, a suicide bomber detonated an IED at an Ariana Grande concert in Manchester. 23 people died, including the attacker. Hundreds of people were wounded, more than half of them children. The attacker was an Islamic fundamentalist.

The Pacific region is one that is changing rapidly, due to increased focus from countries other than traditional Pacifica partners, as well as intensifying trans-national crime and climate change, which has a disproportionate impact on small, low-lying islands.

In addition to providing support in the form of traditional humanitarian assistance and disaster relief, one of New Zealand's top national security priorities is working to improve the safety and security of the Pacific. We do this through allaying debt-diplomacy, assisting in the running of free and fair elections, and providing training and information to public service departments.

As Minister of Justice, I have a keen interest in ensuring our elections are run in a free and fair manner. I am interested in hearing about all of your experiences in this area, as we look to prepare for local body elections in the coming months, and our general election in 2020.

Our geographic isolation, traditionally a protection for us, offers little protection against modern threats, which is why we have recently released a new cyber security strategy, which details the opportunities and risks which new technologies, including artificial intelligence and 5G, will bring.

## **Conclusion**

In conclusion, I look forward to a fruitful two days of discussions, and to collaborating to ensure that our countries remain free, safe, and secure.

We will cover many high-priority policy issues and it is testament to the ongoing strength of this partnership that our discussions will be vigorous and substantive.

'Waiho i te toipoto, kaua i te toiroa' – let us keep close together, not wide apart.

Nga mihi nui - thank you all

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

### Agenda item A: Threat assessments: Counter terrorism

Lead country: s6(a)

#### Talking points

- It will take some time for New Zealand (NZ) intelligence and security agencies to fully understand the long-term implications of the 15 March attack. Understanding the terrorism threat posed by those adhering to an extreme right-wing ideology is a priority for NZ, although the Islamist extremist community also continues to pose a threat.
- NZ is now 'on-the-radar' with extremist groups in a way we haven't previously been. This could possibly result in an increased number of threats against New Zealanders and NZ interests internationally, as well as potential travel by extremist actors to NZ.
- While our recent focus has been on the use of firearms as a weapon, we remain cognisant of the popularity and lethality internationally of less sophisticated attack methodologies.
- Extreme right-wing and Islamist extremist propaganda originating from overseas, and spread using the internet, will continue to be a key factor in the radicalisation of individuals in New Zealand.
- Due to the large volume of New Zealanders living or travelling overseas, we assess the greatest terrorist threat to New Zealanders is incidental harm associated with attacks offshore. However, this does not preclude New Zealanders being deliberately targeted in New Zealand or offshore in the post-Christchurch attack threat environment.
- While much smaller in total numbers than partner nations, the immediate and long-term threat posed by returning foreign fighters and other extremist travellers remains of interest to NZ.

#### Threat Assessment: Counter terrorism

The Threat assessment provides s6(a) perspectives on a suite of security issues, including counter terrorism. No outcomes from this session are proposed. s6(a) paper will be used as the basis for discussion between Ministers during which views can be exchanged on the threats experienced in our respective countries.

RESTRICTED

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

### Background

- On 15 March 2019, the NZ National Terrorism Threat Level was raised from low to high. This followed the events in Christchurch and resulted from a large number of uncertainties related to the attacks, including the potential for further attacks.
- On 17 April 2018\*, the NZ National Terrorism Threat Level was revised from high to medium. This was the result of a greater understanding of the alleged perpetrator of the 15 March attack, individuals and groups adhering to extreme right-wing ideologies, and the Islamist extremist threat in the post-15 March threat environment.
- It will take some time for NZ intelligence and security agencies to fully understand the long-term implications of the 15 March attack. Understanding the terrorism threat posed by those adhering to an extreme right-wing ideology is a priority for New Zealand, although the Islamist extremist community also continues to pose a threat.
- The NZ extreme-right wing community remains fragmented and disorganised, which challenges efforts to identify and assess potential threats.
- The use of online spaces by those adhering to an extreme right-wing ideology is of particular interest, as it allows individuals to radicalise without being detected through internationally-focused sites and social media platforms. Following the Christchurch attack, NZ has featured prominently in extremist propaganda, including both extreme right wing and Islamist extremist (ISIL and AQ).
- While right-wing extremist and Islamist extremist threats are the primary counterterrorism challenge to NZ, there is an awareness of the potential terrorism threat posed by other extremist actors (i.e. other ideologies and issue motivated actors).

### *Status of the Islamic State of Iraq and the Levant (ISIL)*

- We agree that ISIL's global branches and networks have become increasingly important to driving ISIL's narrative. We note there has been an increased frequency of ISIL official media acknowledging affiliates and claiming attacks by its global affiliates – particularly in Africa and South Asia.
- However, ISIL is also clearly seeking to set the conditions of a long-term resurgence in the Middle East. Few of the social, economic, and political factors that contributed to their rise have been addressed and ISIL retains thousands of members and vast sums of money to drive future operations in Iraq and Syria.
- ISIL propaganda continues to be produced and circulated, and their narrative continues to resonate with Islamist extremists in the West. While there has been a

RESTRICTED

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

significant decline in successful ISIL attacks (whether these are directed, enabled, or inspired) in the West, attacks and disruptions continue to occur.

*Status of al-Qa'ida (AQ)*

- AQ remains a concern for NZ, particularly due to their historical intent and capability to target civil aviation but also because AQ-affiliated groups have continued to have significant successes in Africa.
- AQ almost certainly retains the intent to conduct terrorist attacks targeting the West, and AQ is likely to seek to exploit the decline of ISIL to restore and enhance the AQ narrative.
- NZ is concerned about the potential for disillusioned ISIL supporters to switch allegiance to AQ, rather than demobilising or deradicalising.
- We note AQ's strong links to terrorist groups in Southeast Asia and the history of terrorism in this part of the world.

*Threat from returning foreign fighters to NZ*

- While much smaller in total numbers than partner nations, the threat posed by returning foreign fighters and other extremist travellers remains of interest to NZ. This is in terms of both the immediate terrorism threat posed, but also the longer-term impacts of extremist travellers on the NZ community (e.g. radicalisation).
- Challenges returning foreign fighters pose to NZ include the potential for onward travel to other conflict areas, difficulties in prosecuting individuals for crimes committed abroad, and the government-wide resource commitment required to identify and monitor such individuals.

**Papers:**

- Threat assessment: Counter terrorism.

*Combined Threat Assessment Group, NZSIS*

18 July 2019

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## **Agenda item C: Threat assessments: Serious organised crime threats**

**Lead country:** s6(a)

### **Talking points**

- New Zealand (NZ) shares similar threat trends and patterns s6(a), having observed similar recent changes in organised crime threats.
- A Government priority for NZ is the development of a national, multiagency transnational organised crime (TNOC) strategy that will focus on both supply-side issues and demand-side social harms and impacts.
- This strategy will take a 'whole system' approach, including improving governance, coordination, and capability, s6(a)
- s6(a)
- NZ has observed the following organised crime trends:
  - seizures of finished methamphetamine continue to increase
  - demand for cocaine also appears to be increasing
  - s6(a) as the main methamphetamine export country appears to be shifting

### **Threat Assessment: Serious organised crime threats**

The threat assessment agenda item provides s6(a) perspective on a suite of security issues, including organised crime threats. No outcomes from this session are proposed. s6(a) paper will be used as the basis for discussion between Ministers during which views can be exchanged on the specific degree of threats experienced in our respective countries.

### **Background**

- Combating TNOC is a Government priority for NZ. Within NZ, the Senior Managers Forum (the operational multi-agency group focused on transnational organised crime) have identified the seven focus areas as: importation and manufacture of illicit drugs; people trafficking and modern-day slavery; organised crime engaged in business; transnational organised crime groups; professional facilitators and enablers; bribery and corruption; and money laundering.



## RESTRICTED



MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT  
HĪKINA WHAKATUTUKI



DEPARTMENT OF THE  
PRIME MINISTER AND CABINET  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- New Zealand (led by NZ Police) is developing a national, multi-agency Transnational Organised Crime (TNOC) strategy as part of Cabinet's Social Wellbeing Committee Organised Crime work programme.
- The TNOC strategy has a particular focus on supply-side issues, while also having a strong emphasis on demand-side social harms and impacts. As part of this process, NZ Police is updating our national TNOC Risk Assessment, which was last updated in May 2016.
- Our draft TNOC strategy aims to take a 'whole system' approach, including improving governance, coordination, capability, and focusing on the cross-cutting impacts of TNOC. It prioritises the highest harms impacts of OCGs and networks, regardless of the crime type. The strategy is underpinned by strengthened system resilience for the ultimate aim of protecting businesses, the public and the most vulnerable.
- Overall, NZ is well-placed to combat a broad range of criminal offending committed by TNOC groups. We work in a number of forums focusing on TNOC, both nationally and internationally, using a variety of approaches.

### *Threat trends and patterns*

- NZ has observed the following organised crime trends:
  - **Seizures of finished methamphetamine continue to increase**, indicating high national demand.
  - **Demand for cocaine also appears to be increasing**, and the high market price that it commands domestically makes New Zealand an attractive destination for overseas suppliers.
  - s6(a) **as the main methamphetamine export country appears to be shifting.** 6(a)

RESTRICTED



s6(a), 6(b)(i)

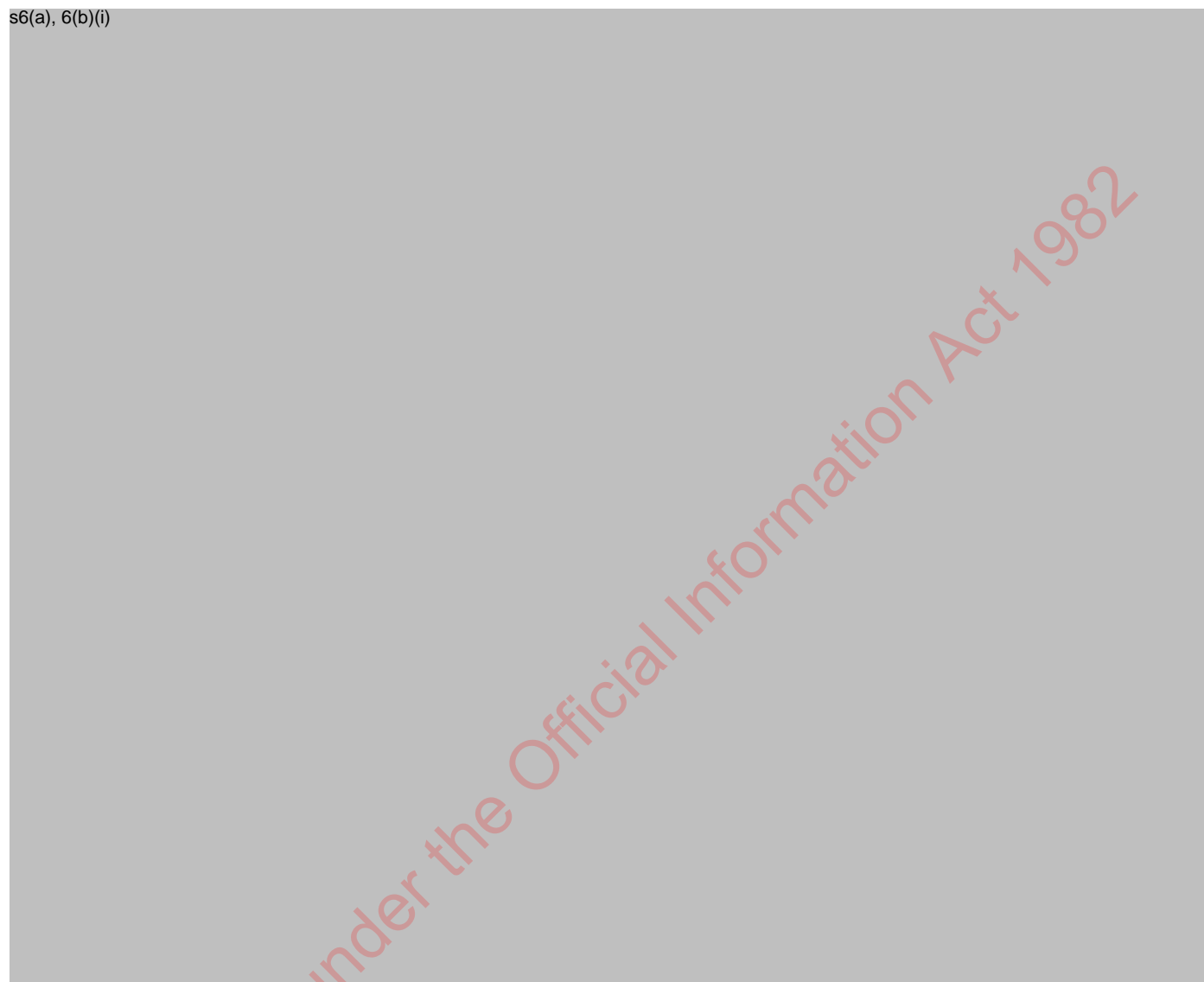


### *Challenges*

- **Organised crime groups exploit opportunities that arise from globalisation**, particularly using increased legitimate trade and travel flows to obscure criminal activity. They display a high level of adaptability and are increasingly agile and fluid in the face of disruption efforts.
- **New communication technologies** (e.g., applications with end-to-end encryption) make it difficult for Police and intelligence agencies to successfully intercept and disrupt OCG networks.



s6(a), 6(b)(i)



### *Opportunities*

- Countries acting in partnership will be better able to counter TNOC groups and leverage influence with key partners. Alignment, expertise and information sharing and could be improved between countries to stay one step ahead of TNOC networks, many of which utilise sophisticated technology, encryption, and tradecraft.
- Successful reintegration is needed to prevent reoffending by deportees. A cross-agency wraparound approach would assist with deportee reintegration, along with extensive services for deportees who are high risk and have high needs, particularly in relation to alcohol and other drugs, mental health, and stress management.

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

• s6(a), 6(b)(i)

**Papers:**

- Threat assessment: Serious organised crime.

*New Zealand Police*

18 July 2019

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## **Agenda item D: Threat assessments: Asylum trends**

**Lead country:** s6(a)

### **Talking points**

- Relative to our five country partners, New Zealand (NZ) has low numbers of asylum claims (over the period 2016 – 2019 we received 1382 claims).
- While the number of claims is increasing, this is relative to the general increase in the number of temporary arrivals into NZ.
- We are not aware of large-scale *systematic* criminal involvement in the asylum process in NZ, however in the past year we have become aware of potential organised fraudulent activity in relation to some claims from Asia.
- We are aware of the situations that s6(a) has highlighted regarding assertions of false religious beliefs or sexual orientation, however, standard interview, investigation and credibility assessments, along with modern investigation techniques, are usually able to address these cases where they occur in NZ.
- NZ employs most of the tools to detect potential fraud which s6(a) has described. Technological advancements in identity matching and document diagnostics have provided additional tools to assist in detecting fraud. However, in NZ our most important tool in detecting fraud is well-trained and competent staff.
- The fact that asylum claims are low and decision-making is handled by one office in NZ, also limits opportunities for fraud. NZ generally has excellent records on migrants, visas and travel, and access to this information is useful in detecting false claims.
- We are aware that the advent of electronic communications, the internet and social media have created opportunities for false claims and fraudulent activity. However, these technologies also offer opportunities for investigation and fact checking. Access to social media and prompt and reliable verification channels have improved decision-making in NZ.
- Information available through five-country collaboration is often relevant and useful to NZ's management of asylum claims, and any efforts to further such collaboration would be supported.



## **Threat Assessment: Asylum trends**

The Threat assessment provides <sup>s6(a)</sup> perspective on asylum trends. No outcomes from this session are proposed. <sup>s6(a)</sup> paper will be used as the basis for discussion between Ministers during which views can be exchanged on the specific degree of threats experienced in our respective countries.

## **Background**

- NZ has a low number of asylum claims and a thorough and considered process for determining whether claims are genuine.
- While the number of refugee and protection claims lodged in NZ has steadily increased over the last few years, the origin of the increase appears to be a general across-the-board increase in temporary arrivals into NZ. There is no discernible pattern of claim type, nationality, visa type or travel method.
- In 2016-17, there were 434 claims, 229 of which were declined; in 2017-18 there were 438 claims, 281 of which were declined; in 2018-19 there were 510 claims, 284 of which were declined. Of the 1382 claims received over the period 2016 to 2019, 794 were declined, but only 12 were determined to be 'manifestly unfounded'.
- The majority of people who claim refugee status in NZ have entered the country on valid travel documents—on a visa either granted offshore or at the border (for those that are visa-free). In addition, around 40-50 per cent lodge their claim after living in NZ for 12 months or more.
- A small number of people claim at the border on arrival and a small proportion of those may be refused entry to NZ for reasons relating to identity, security or criminality. Asylum seekers who have been refused entry to NZ are detained under a court reviewed Warrant of Commitment at the Mangere Refugee Resettlement Centre or a penal facility. While their claim is being determined, the level of restriction on their movements may be changed, including being released on conditions into the community.

## ***Exploitation of NZ's asylum system***

- There is no evidence that NZ's asylum system is being *systematically* abused either by people claiming asylum or by criminal networks trying to exploit vulnerable migrants, although there have been two cases in the past year that indicate potential criminal involvement in the asylum process. The first of these cases (<sup>s6(a)</sup>) has been addressed by Immigration New Zealand and the fraudulent activity has been



**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

shut down, while the second case (s6(a)) is currently under consideration.

*Work in NZ to address potential fraud in the asylum process*

- Exploitation of asylum systems is not a new phenomenon, and the assertion of false religious beliefs or sexual orientation is well known to asylum decision-makers in NZ. Standard interview, investigation and credibility assessments, in tandem with modern investigation techniques, are usually able to address such concerns.
- s6(a)
- Well-trained and competent staff, however, are considered to be the key factor in detecting false claims.
- The fact that asylum claims are low in number and decision-making is handled by one office in NZ also limits opportunities for fraud.
- The advent of electronic communications, the internet and social media have created opportunities for false claims. However, these technologies also offer opportunities for investigation and fact checking previously unknown to decision-makers. Access to social media and prompt and reliable verification channels have improved asylum decision-making in NZ.
- New Zealand law also allows disclosure of claimant information in order to determine the claim or maintain the law. NZ decision-makers may make inquiries or seek information from sources in third countries or even the country of origin, if it is reasonable and safe to do so. NZ decision-makers work to publish guidelines on this process that include discussing the proposed inquiry with the claimant in advance.
- Information available through five-country collaboration is often relevant and useful, and any efforts to further such collaboration would be supported.

*The asylum system in New Zealand*

- Asylum seekers are usually represented by a lawyer and have access to interpreters. They have numerous opportunities to establish their claim (through a claim form, written statement, interview, and legal submissions) and most are able to do so and effectively participate in the process.

**RESTRICTED**

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- Other than subsequent claims and those made in bad faith, NZ does not proscribe or limit claims from any nationality or class of person.
- The legal system has a low standard of proof (a 'real chance') and extends the benefit of the doubt to claimants who are otherwise credible but unable to "prove" or provide independent evidence of their claim.

### *Legislative context*

- New Zealand is a signatory to international conventions that support the right of people to claim asylum in New Zealand. The relevant conventions and covenant are: the 1951 Convention Relating to the Status of Refugees; the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment and the 1966 International Covenant on Civil and Political Rights.
- In New Zealand, asylum claims are decided according to the Immigration Act 2009 (Section 5). One of the purposes of the Immigration Act 2009 is to ensure that New Zealand meets its obligations in relation to the above conventions and covenant.
- In support of these obligations, New Zealand has a robust refugee protection framework that is both accessible and manages the risks associated with potential fraud or security, while at the same time recognising those that need protection.
- In NZ, two authorities are responsible for determining refugee status:
  - At first instance, the Immigration New Zealand Refugee Status Branch undertakes processing and determination of refugee and protected person claims.
  - At appeal, decline decisions can be appealed to the Immigration and Protection Tribunal (an independent tribunal within the Ministry of Justice), which hears the case anew.
- Interviews are an important feature of the New Zealand system of determining refugee status and are key to testing the basis of claim as well as assessing credibility and identifying specific matters to be addressed. Alongside interviews, country research is utilised and other security checks are undertaken, including the collection and sharing of biometrics with our Migration Five partners.

**RESTRICTED**

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- The Immigration Act allows refugee decision-makers to consider information “from any source”. For example, it allows social media to be considered, and it does not lay down “rules of evidence”. Administrative law principles of fairness and natural justice must still be applied such that the decision-maker must reasonably determine what weight the information should be given, and must provide any prejudicial information to the person in advance for comment. [Note: legislative provisions for the use of classified information are exceptions to these rules.]
- New Zealand law also allows disclosure of claimant information in order to determine the claim or maintain the law. NZ decision-makers may make inquiries or seek information from sources in third countries or even the country of origin, if it is reasonable and safe to do so. NZ decision-makers work to publish guidelines on this process that include discussing the proposed inquiry with the claimant in advance.
- Under the provisions of the Immigration Act, officers making decisions on asylum claims are able to review refugee decisions and cancel or cease recognition and deport a refugee who is a danger to the community in NZ or a risk to national security. These provisions are actively used and serve to ensure the integrity of the refugee system and to protect NZ.

### Papers:

- Threat assessment: Asylum trends

*Immigration New Zealand, Ministry of Business Innovation and Employment.*

12 July 2019

RESTRICTED



## Agenda item 1; 1a: Cyber - Current Threats and Response

Lead country: s6(a)

### Talking points

- New Zealand networks face a range of increasingly advanced and numerous cyber threats, from both state and non-state actors – the global threat landscape is our threat landscape. While we fortunately avoided the impacts of campaigns like WannaCry or NotPetya others such as Cloudhopper have affected us.
- s6(a)
- New Zealand's recently released cyber security strategy highlights the importance of international partnerships, such as this forum; protecting national security; and, respecting human rights online, which is critical in allowing us the social licence to respond to actors who do not hold these values.
- New Zealand values coordinated responses to malicious cyber activity. In our view, the broader the group willing to act, the better we reinforce norms of responsible state behaviour online. s6(a)
- New Zealand's security sector will continue to work closely with its Five Eyes counterpart agencies to strengthen the long-standing cooperation arrangements we have to respond to cyber incidents and manage risks.

s6(a), 6(b)(i)



s6(a), 6(b)(i)

## **Background**

5. New Zealand remains a target for a range of state and non-state actors. In 2018 we saw a nearly 10% increase in detected incidents which had characteristics similar to known state actors compared to the previous year. This mirrors similar increases in other Western states. States target New Zealand networks to raise revenue, meet espionage requirements, or for valuable intellectual property.
6. New Zealand's NCSC recorded 347 cyber security incidents in the reporting year from 1 July 2017 to 30 June 2018. 134 of these incidents (39 percent of the total) contained indicators that had been linked to known state-sponsored cyber actors.
7. CERT NZ continues to experience substantial increases in reported incidents and financial losses from businesses and individuals since its establishment in 2017. Most

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

recently, in Q1 2019, 992 incident reports were received in Q1, the second highest number of reports received after Q4 2018. Scams and fraud made up 75% of financial losses in the quarter and unauthorised access reports reached their highest number to date, increasing 19% on Q4. This is linked to increases in business email compromises affecting more New Zealand organisations.

8. s6(a)

[Redacted]

9. States are increasingly also affected by non-traditional cyber threats. Authoritarian states frequently use disinformation campaigns to quell domestic audiences and to influence events in other states. s9(2)(g)(i)

[Redacted]

10. A protocol was put in place before the last general election to set out the NZSIS and GCSB's roles in responding to foreign state threats and cyber and cyber-security threats to the election. It was not activated.

11. An increasing number of states are openly developing offensive cyber capabilities, which is creating a more contested cyberspace as they seek to use their new capabilities. s6(a)

[Redacted]

**Papers:**

- Cyber – Current Threats and Responses s6(a)

*National Cyber Policy Office*

*Department of the Prime Minister and Cabinet*

*July 2019*

**RESTRICTED**





## Agenda item 1B: Cyber Threats - 5G

Lead country: s6(a)

### Talking points

- New Zealand sees the security of 5G networks as critical, given their key future role in fostering economic growth and future wellbeing. Our legislation, the Telecommunications (Interception Capability and Security) Act, provides an effective risk based framework for mitigating network security risks that is country of origin and vendor neutral.

• s6(a)

•

•

s6(a), 6(b)(i)

~~RESTRICTED~~



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

- Released under the Official Information Act 1982
6. As you are aware, the GCSB declined an application from Spark in November 2018 to build a 5G ready network that included Huawei technology.
  7. New Zealand has undertaken a policy process to test whether TICSAs can mitigate network security concerns arising from 5G networks. Officials have determined that TICSAs are fit for purpose and successfully mitigate network security risk. They will not recommend legislative changes.
  8. We are confident in the ability of TICSAs to provide appropriate network security for New Zealand. But we are mindful that 5G will evolve, and bring with it a raft of new security challenges. To this end we welcome ongoing discussions on best practice and technical details. We are grateful for the cooperation on these issues to date.

~~RESTRICTED~~

~~RESTRICTED~~



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

Released under the Official Information Act 1982

~~RESTRICTED~~

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**

~~RESTRICTED~~



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

Released under the Official Information Act 1982

~~RESTRICTED~~

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

**Papers:**

- Position Paper: 5G

- s6(a)

*National Cyber Policy Office*

*Department of the Prime Minister and Cabinet*

*July 2019*

**RESTRICTED**





## **Agenda item 2A: Emergent technologies: Trusted Markets for Critical and Emerging Technologies**

**Lead country:** s6(a)

### **Talking points**

- New Zealand supports the Five Eyes goal of an open, diverse and competitive international technology market.
- Collaborating between likeminded countries is key for achieving this goal of trusted markets.
- Supply chain security is also an important component of trusted markets. These issues will only become more important as digital technology becomes more integrated into our societies and economies.
- We must also, however, be mindful that increased interstate competition in the international technology market could have unforeseen negative consequences. We must ensure we balance trade obligations and economic considerations with national security.

s6(a), 6(b)(i)



## Advice

1. This item should be read in conjunction with the IoT and 5G papers, given the significant overlap between these items.

### *New Zealand supports greater collaboration on security and market diversity*

2. Promoting security by design<sup>1</sup> in networked devices is important for building a free, open and safe digital ecosystem. New Zealand also supports market diversity of technology, particularly in the telecommunications equipment market.
3. Given that modern technology supply chains are global, New Zealand must work collaboratively with our international partners to influence the development of these markets.

s6(a), s6(b)(i)

6. New Zealand supports the inclusion of language in this portion of the communique supporting the development of the IoT Joint Statement of intent.

s6(a), s6(b)(i)

## Background

### *Trusted Markets*

8. Trusted markets, s6(a) refers to the technology market segment. Ideally these markets will be open, diverse and competitive, and able to provide technology with security built in by design.

---

<sup>1</sup> Secure by design means that the hardware and software has been designed from the foundation to be secure, rather than security added later in the development cycle (as is often the case).

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

**Papers:**

- Position paper: Trusted Markets for Critical and Emerging Technologies

*National Cyber Policy Office*

*Department of the Prime Minister and Cabinet*

11 July 2019

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## Agenda item 2a: Internet of Things

Lead country: s6(a)

### Talking points

- The Internet of Things (IoT) is a source of economic opportunity. It also presents significant cyber security risk.
- s6(a)
- There is an intersect with this and international standard setting for IoT security.
- s6(a), 6(b)(i)
- 

s6(a), 6(b)(i)



s6(a)

s6(a), 6(b)(i)

## **Background**

### *What is the Internet of Things?*

7. IoT devices can operate as part of an online network, often transforming the way that everyday functions or industrial processes work. The growth of IoT has been fuelled by the continuous decrease in price for small, powerful microprocessors and network devices, and by ubiquitous connectivity. The analyst firm Gartner predicts that, by 2020, there will be 20.4 billion IoT devices worldwide.

### *IoT is a source of growth and opportunity...*

8. IoT devices have been used in New Zealand industry for years - for example, smart power and gas meters in the power sector. Non-consumer IoT is spreading in many other industries - internet enabled devices are increasingly used in farming to check soil quality

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

and water levels. For governments, cities with large sensor networks may bring many benefits, among them more efficient traffic management to help ease congestion, and energy efficiency from the better use of public goods like street lights. Thus IoT applications and networks provide the means for “smart cities”.

*... but IoT devices also present a security risk.*

9. IoT devices are often developed and produced as quickly and cheaply as possible. Security, if it is added, has generally been added as an afterthought, rather than ‘security by design’ at the beginning of the process. And given the sheer number of devices that will constitute the IoT, this poses a new and unique challenge on a massive scale.
10. The result of this poor security is an increase in attack surface (the number of points a malicious actor can try to access a device or network), with each device representing an entry or exit point to a network or system.
11. Depending on the IoT device, this can result in the theft of private information generated or transmitted by the device, or unauthorised access, control and damage to the devices and the systems to which they are connected. IoT deployment and update will continue to increase the nature and scale of cyber vulnerabilities nationally and globally.
12. New Zealand is a technology and regulation taker and will follow commercial, technology and regulatory trends in IoT. Almost all IoT devices are imported, and while there are firms manufacturing IoT devices in niche economic sectors (like agriculture), there is no large-scale domestic manufacturing of IoT devices. This makes the task of securing the IoT more complex, and necessitates New Zealand working closely with our international partners.

*What is New Zealand doing to secure IoT?*

13. Currently, New Zealand has not yet adopted regulations, mandatory safety or security standards, or government-endorsed security guidelines specifically for IoT device security.
14. The Consumer Protection team within MBIE has released information for consumers that describes some of the risks to consumers from poorly secured IoT devices. The National Cyber Security Centre provides cyber security advice and technical assistance to critical national infrastructure (CNI) entities. This includes advice on the security of IoT devices on the networks of CNI entities. CERT NZ provides general information security advice for the public, much of which is applicable to IoT devices.
15. The National Cyber Policy Office has established an interagency group to explore New Zealand’s options for securing IoT, and how to best contribute to the global efforts

**RESTRICTED**



**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

to promote IoT security. This work crosses over a number of portfolios. These include cyber security, consumer protection, and international regulatory cooperation.

s6(a), 6(b)(i)

**Papers:**

- Internet of Things (IoT)
- Annex: s6(a), 6(b)(i)

*National Cyber Policy Office  
Department of the Prime Minister and Cabinet  
11 July 2019*

**RESTRICTED**

**Five Country Ministerial 2019  
London, 29-30 July**



## **Agenda item 2B: Emerging Technologies: Drones**

**Lead country:** s6(a)

### **Talking points**

- New Zealand supports the outcomes sought by this position paper.
- Drones, like other emerging technologies, present considerable opportunities (for example, innovation) but also challenges that many jurisdictions are grappling to respond to.
- We should leverage our collective experiences to ensure we can capture the full benefits of emerging technologies such as drones, while mitigating their negative impacts.

s6(a), 6(b)(i)

### **Advice**

s6(a), 6(b)(i)

1. Transformative technologies like drones raise a number of challenges for policy-makers, relating to safety, national security, privacy and social acceptance. To maximise the benefits of drone technology while managing the challenges, governments need to be able to move at pace with this emerging sector.
2. Other countries are grappling with similar challenges to New Zealand with respect to drone technology. C-UAS solutions are designed to counter threats from drones, and include technologies like track-and-detect and drone guns. s6(a), 6(b)(i)

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

[Redacted]

3. s6(a)

[Redacted]

s6(a), 6(b)(i)

[Redacted]

4. s6(a), 6(b)(i)

[Redacted]

5. Much of the technology to address the risks posed by drones is being developed by industry.<sup>1</sup> Industry-led solutions will be one of the key building blocks in enabling governments to identify rogue drone operators, and intervene where necessary.

6. s6(a), 6(b)(i)

[Redacted]

s6(a), 6(b)(i)

[Redacted]

7. s6(a), 6(b)(i)

[Redacted]

8. As New Zealand doesn't have a specific national security science and research agency, our participation in the group is coordinated by MBIE, in conjunction with DPMC. There are regular meetings of agencies <sup>s6(a)</sup> [Redacted], including the Ministry, Civil Aviation Authority (CAA) and relevant agencies.

---

<sup>1</sup> s6(a), 6(b)(i)

[Redacted]

**RESTRICTED**

9. s6(a), 6(b)(i)

10.

11.

12.

13.

## **Background**

### *Drones and the aviation system*

13. New Zealand already has robust civil aviation rules in place relating to drones that, if followed, provide for a safe aviation system. However, the nature of drones makes it difficult to identify non-compliant operators, which impedes enforcement and the effectiveness of the rules.
14. The Ministry, supported by the CAA, has developed a regulatory work programme in the short- to medium-term exploring a package of potential interventions to address current and emerging risks from the use of drones. It also aims to enable innovation and development in the drone sector and lay the early groundwork for future integration of drones into the national transport system.
15. While these interventions will assist with improving compliance generally, they are likely to have limited impact on drone operators who are determined to cause harm and who will deliberately circumvent any regulatory requirements or technological safeguards. Other interventions are required to address the risks these operators pose, like C-UAS.

### *There is cross-government interest in drones*

16. Cabinet recently agreed to a vision paper, developed by the Ministry and supported by the CAA, Airways and MBIE, to enable a thriving, innovative and safe drone sector and

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

providing a pathway for the safe integration of small and more advanced drones in New Zealand.

17. The vision paper supports a cross-government multi-year work-programme covering regulation, funding and investment, infrastructure and technology, and research and development.

### *Counter-Unmanned Air Systems*

18. The Ministry is the lead agency to address drone-related security concerns. MBIE has an interest in the emerging drone sector as it is an area of transformative technology and is research and development intensive.
19. A blended suite of capabilities, readiness activities, technology and commercial solutions are needed to create a holistic C-UAS solution with detection and intervention capabilities. The supply of “ready to go” C-UAS technology and capacity in the market internationally is limited, and the lead-in time for manufacture could be significant. There are also practical difficulties with this technology, such as the risk to public safety if a drone is ‘shot’ down, or the risk to other aircraft if radiofrequencies are jammed.
20. MBIE aims to support not only the testing and development of advanced drones, but also adjacent technologies which may include C-UAS equipment. Airways has been trialling different drone detection systems at Auckland Airport, focused on detecting drone activity in the vicinity of the Airport for aviation safety purposes. While some of these systems show promise, it is clear that at this stage, no single system is entirely effective at identifying and tracking drones.

### **Taking Flight: Drones vision paper**

#### *Purpose of the paper*

21. Taking Flight sets out a cross-government vision for the integration of drones into the aviation system and the wider transport sector.

#### *What the paper says*

22. The paper says that New Zealand is regarded as being at the forefront of drone development due to our enabling regulations for drone flights that fall outside of standard parameters.
23. To maintain our position at the forefront of drone development, we need to provide clarity to the drone sector and the general aviation sector about the government’s vision for drones.

**RESTRICTED**

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

24. Taking Flight confirms that drone integration is a cross-government goal in New Zealand. It goes on to define successful integration as a time when the drone sector is thriving, safe, and innovative. It then sets out that integration will rest on the four building blocks of regulation, research and development, investment and funding, and infrastructure and technology.
25. The paper also provides examples of how drones could be used in the future, and provides an illustration of the usage of airspace by drones and general aviation.
26. The paper also outlines the agencies that are involved in the drone integration work, and details the UA Leadership Group established by the Ministry of Transport.

### *Benefit Study*

27. Taking Flight was released alongside the Drone Benefit Study, which was commissioned by Ministry of Transport and Ministry of Business, Innovation, and Employment.
28. The study tried to quantify the impact that drones could have on different sectors of the New Zealand economy, based on literature reviews, modelling, and stakeholder interviews.
29. The study found that almost all sectors of the economy could benefit from drones to some extent. However, our primary industries are the main candidates for improvement.
30. The total value of all the benefits over the next 25 years could be as high as \$7.9 billion.

### *Next Steps*

31. The next steps are the implementation of the vision and aligning the ongoing work to the vision. Current work includes:
- a. MOT led- Investigation of new regulatory options for drones
  - b. MOT led- Industry engagement with drone and aviation sectors
  - c. MOT led- Social outreach on our work
  - d. MOT led- Initial policy investigation on unmanned traffic management in New Zealand
  - e. MBIE led- Work on integration trials and establishing drone development test sites
  - f. CAA led- Continue education campaigns for drone users

**RESTRICTED**



**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- g. CAA led- Continue engagement with commercial operators seeking Part 102 certificates for drone flights/equipment exceeding standard parameters

**Papers:**

- Position paper: Counter-Unmanned Air Systems (C-UAS).

*The Ministry of Transport*

11 July 2019

Released under the Official Information Act 1982

**RESTRICTED**



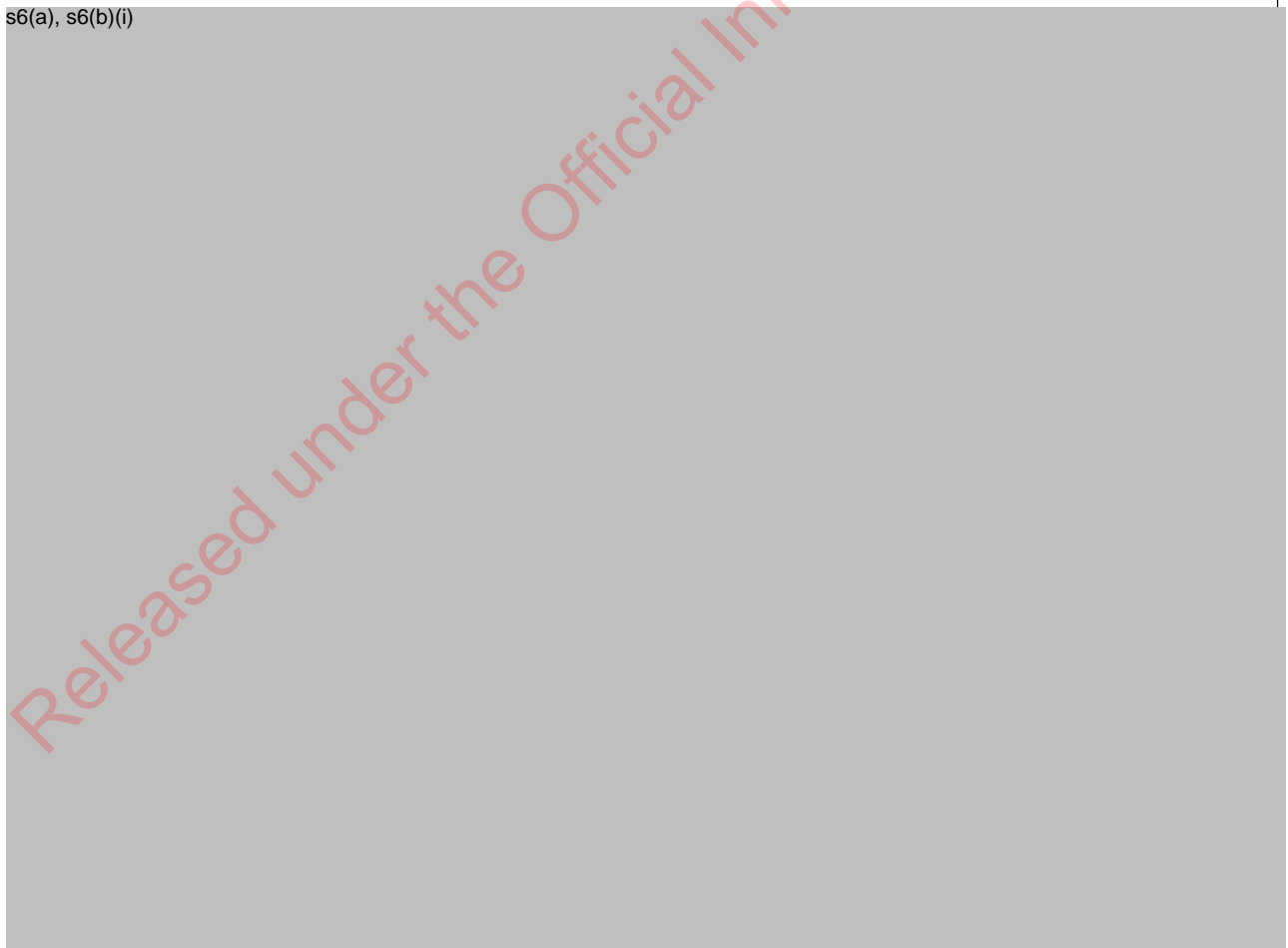
## **Agenda item 3 A: Asylum system abuse and fraud**

**Lead country:** s6(a)

### **Talking points**

- New Zealand (NZ) takes its international commitments seriously in relation to providing protection to those who are found to be in need of that protection.
- We have a robust and accessible asylum system that manages immigration risks, while also recognising those who need protection.
- There is always a risk of fraudulent activity in relation to asylum claims s6(a), 6(b)(i)

s6(a), s6(b)(i)



**RESTRICTED**

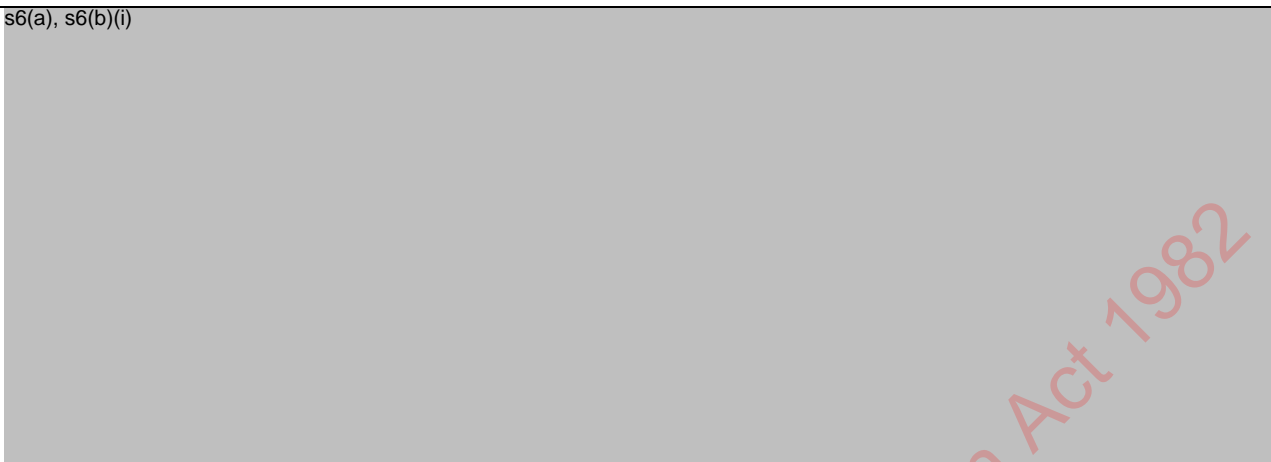


**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI

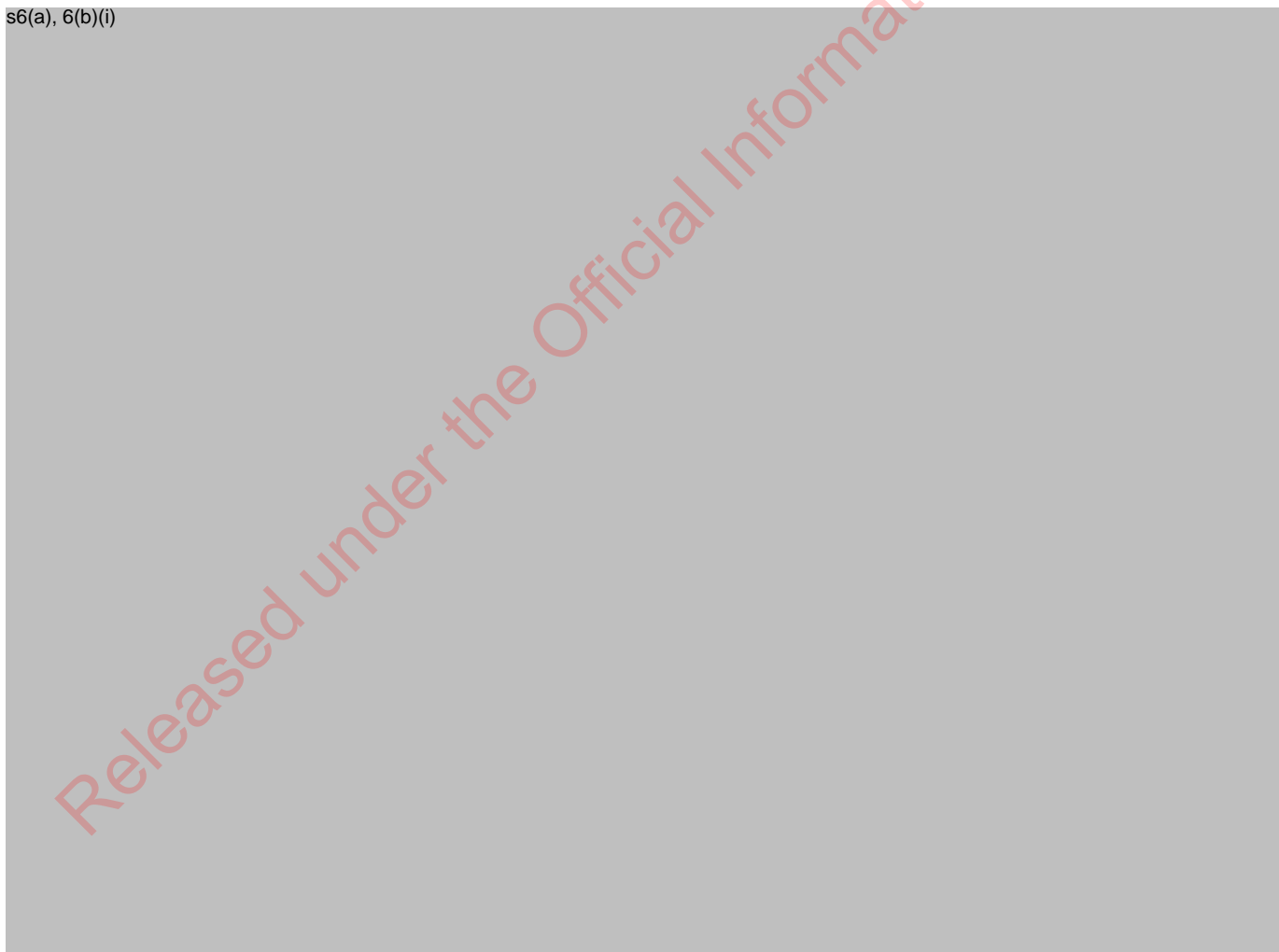


**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)



s6(a), 6(b)(i)



**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**

**RESTRICTED**

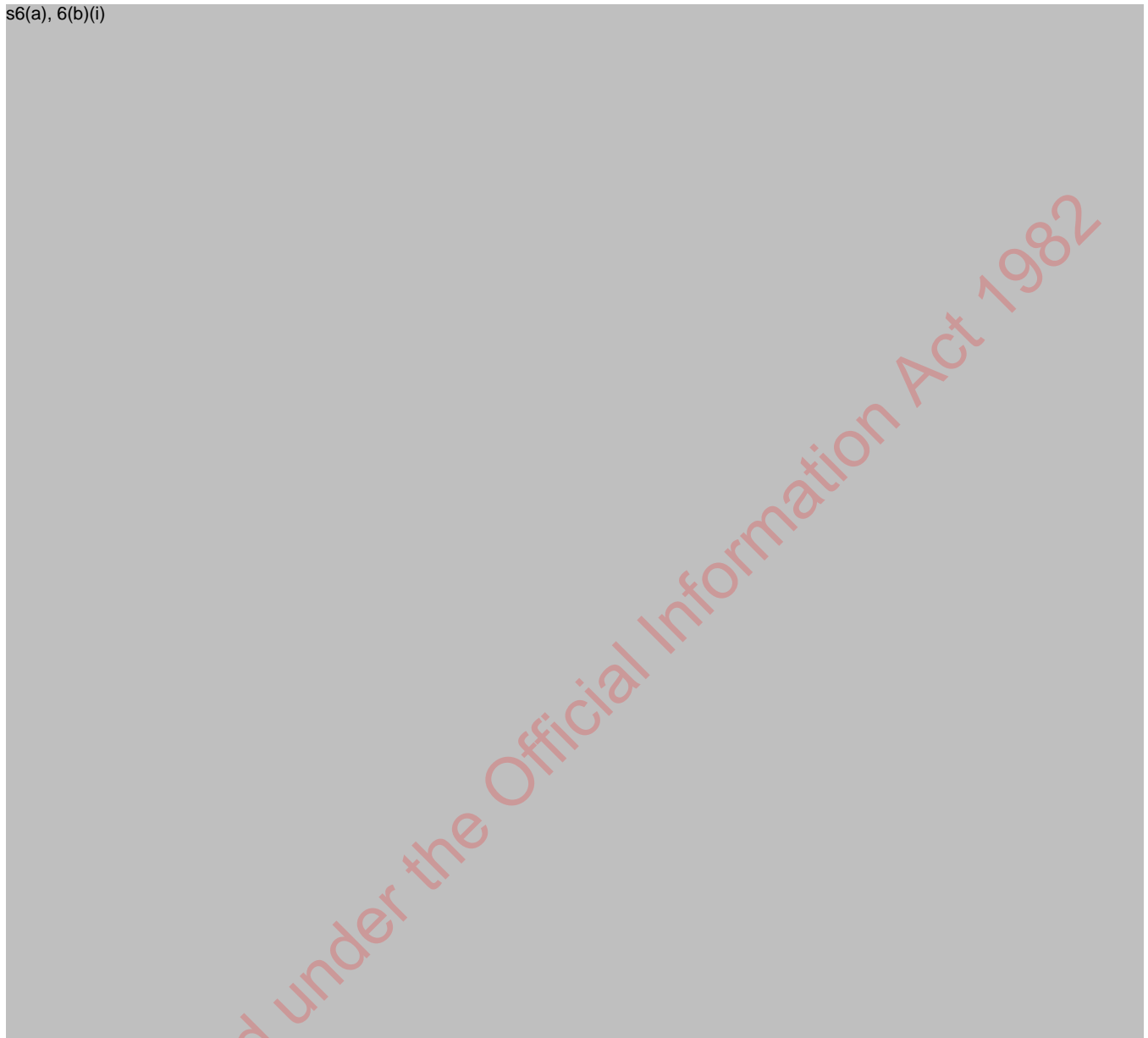


**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)



*New Zealand already has systems in place to address irregular migration*

- People claiming refugee status subject themselves to extensive scrutiny through both the Refugee determination process and security assessments. We therefore consider that, given that criminal third party actors are almost certainly involved in other immigration related fraud or people smuggling, strengthening efforts across the five countries to combat irregular migration should also be effective in addressing organised criminal activity in relation to asylum seekers.
- As a result of its successful 2019 Mass Arrivals Prevention Strategy budget bid, Immigration New Zealand (INZ) is looking to establish an open source intelligence capability through recruitment and investment in open source and social media

**RESTRICTED**

## RESTRICTED



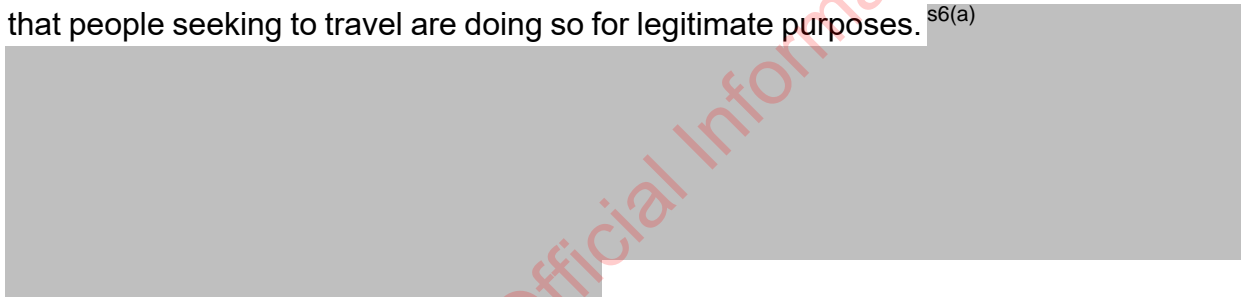
**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

technologies. This will enable the proactive monitoring of open source information and social media in relation to maritime people smuggling.

- Additionally, INZ's Country Research Branch provides open source research support for investigations into people smuggling and facilitation, and responds to requests for country of origin information by Refugee and Protection Officers, to support the refugee status determination process. Through participation in Ministry of Business, Innovation and Employment open source working groups, INZ is developing training, assessing technologies and supporting social media intelligence practitioners with the aim of strengthening INZ's overall capability to address irregular migration through social media intelligence gathering. Additionally INZ's Refugee Status Branch reviews social media content when considering asylum cases.
- The paper proposes that Ministers agree to explore coordination of capacity building and ways to encourage other countries to strengthen visa policies and practices to ensure that people seeking to travel are doing so for legitimate purposes.<sup>s6(a)</sup>



### **Background - Refugee and protected person processes in New Zealand**

#### *Legislative context*

- NZ is a signatory to international conventions that support the right of people to claim asylum in NZ. The relevant conventions and covenant are: the 1951 Convention Relating to the Status of Refugees; the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment and the 1966 International Covenant on Civil and Political Rights.
- In NZ, asylum claims are decided according to the Immigration Act 2009 (Section 5). One of the purposes of that Act is to ensure that NZ meets its obligations in relation to the above conventions and covenant.
- In support of these obligations, NZ has a robust refugee protection framework that is both accessible and manages the risks associated with potential fraud or security, while at the same time recognising those that need protection.

**RESTRICTED**



## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- NZ has two authorities that are responsible for determining refugee status:
  - At first instance, the INZ Refugee Status Branch undertakes processing and determination of refugee and protected person claims.
  - At appeal, decline decisions can be appealed to the Immigration and Protection Tribunal (an independent tribunal within the Ministry of Justice), which hears the case anew.
- Interviews are an important feature of the NZ system of determining refugee status and are key to testing the basis of claims as well as assessing credibility and identifying specific matters to be addressed. Alongside interviews, country research is utilised and other security checks are undertaken, <sup>s6(a)</sup> [REDACTED].
- The Immigration Act allows refugee decision-makers to consider information “from any source”. It allows, for example, social media to be considered and does not lay down “rules of evidence”. Administrative law principles of fairness and natural justice must still be applied such that the decision-maker must reasonably determine what weight the information should be given, and must provide any prejudicial information to the person in advance for comment. [Note legislative provisions for the use of classified information are exceptions to these rules.]
- NZ law also allows disclosure of claimant information, in order to determine the claim or maintain the law. NZ decision-makers may make inquiries or seek information from sources in third countries or even the country of origin, if it is reasonable and safe to do so. NZ decision makers work to published guidelines on this process that include discussing the proposed inquiry with the claimant in advance.
- Under the provisions of the Immigration Act 2009, officers making decisions on asylum claims are able to review refugee decisions and cancel or cease recognition, and deport a refugee who is a danger to the community in NZ or a risk to national security. These provisions are actively used, and serve to ensure the integrity of the refugee system and to protect NZ.

### *Current review*

- An independent review is being undertaken of the first instance determination process, to explore how it could be more effective and efficient and ensure that the information

**RESTRICTED**

## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

required to make a determination is available from the earliest stage. The findings and recommendations of the report will support changes to the process in the future.

### *Situation of claimants*

- The majority of people who claim refugee status in NZ have entered the country on valid travel documents on a visa either granted offshore or at the border (for those that are visa-free). In addition, around 40-50 per cent lodge their claim after living in NZ for 12 months or more.
- A small number of people claim at the border on arrival and a small proportion of those may be refused entry to NZ for reasons relating to identity, security or criminality. Asylum seekers who have been refused entry are detained under a court reviewed Warrant of Commitment at the Mangere Refugee Resettlement Centre or a penal facility. While their claim is being determined, the level of restriction on movement may be changed, including being released on conditions into the community.

### *Numbers of refugee claims*

- The number of refugee and protection claims lodged in New Zealand has steadily increased over the last few years, however the origin of the increase appears to be a general across-the-board increase in temporary arrivals into New Zealand.
- There is no discernible pattern of claim type, nationality, visa type or travel method. In the 2016 -17 financial year there were 434 claims, of which 229 were declined; in 2017-18 there were 438 claims, of which 281 (64%) were declined, in 2018-19 there were 510 claims, of which 284 (56%) were declined. Of the 1382 claims received over the period 2016 to 2019, 794 (57%) were declined, but only 12 were determined to be 'manifestly unfounded' (0.09%).

### *The Global Compact on Refugees*

- Australia, Canada, NZ and the United Kingdom are signatories to the Global Compact on Refugees.
- The Global Compact on Refugees (Refugee Compact) was a process led by the United Nations High Commissioner for Refugees (UNHCR) with views sought on the text from member states and other international organisations through six rounds of consultations in Geneva, which concluded in July 2018.
- With refugee populations increasing, resettlement places being reduced by 50 per cent and the UNHCR budget facing an approximate 40 per cent shortfall, the Refugee Compact establishes a plan of action for international cooperation to assist refugee

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

populations and the international community (particularly hosting states) to manage large scale refugee crises.

- The Refugee Compact is non-binding and sets out how expertise and resources should be mobilised. It proposes a number of measures to better share responsibility and cooperate in order to manage large-scale movements of refugees (including through, for example, expansion of and innovative partnerships, increasing resettlement opportunities for refugees through resettlement programmes and complementary protection, and expanding protection space so that refugees can access legal employment, housing, health care and education).
- At the end of 2018, the Refugee Compact was affirmed at the United Nations (UN) in New York through the UNHCR Omnibus resolution. NZ joined the majority of UN member States in affirming the resolution. The United States was the only State to vote against the resolution and three countries abstained (Libya, Liberia and Eritrea).
- The Refugee Compact established a Global Forum on Refugees as the main vehicle to mobilise support for refugee issues. The Forum is to be held, at Ministerial level, every four years. At the Forum, donor States will be encouraged to make pledges in support of the Refugee Compact – these could include financial assistance, resources and expertise or resettlement places. The first Global Forum on Refugees will be held in Geneva on 17-18 December 2019.

**Papers:**

- Asylum systems abuse and fraud

*Immigration New Zealand*

*Ministry of Business, Innovation and Employment*

17 July 2019

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## **Agenda item 3 B: Data sharing**

**Lead country:** s6(a)

### **Talking points**

s6(a), 6(b)(i)

- [Redacted]
- [Redacted]
- NZ uses a 'privacy by design' approach to the development of IT systems, applications and business practices, proactively embedding privacy into their design and operation.
- For the purposes of facilitating people and trade across our border, we prefer an approach where individuals authorise the sharing of their personal data for a specific purpose. This should be in the full knowledge of what data is being collected, how that data will be used, and where, and for how long, it will be stored.

s6(a), 6(b)(i)

- [Redacted]
- In light of the events on 15 March 2019 in NZ, an independent Royal Commission of Inquiry has been established, and I anticipate that it is likely to look at such things as the collection, sharing and use of information to protect the community, including border and traveller information.
- Last year we consulted publicly on the creation of an Electronic Travel Authority which will involve the collection and long term storage of information on many travellers. Relatively few concerns were raised in response to the proposal.

s6(a), 6(b)(i)

• [Redacted]

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

- 
- 
- 



Released under the Official Information Act 1982

s6(a), 6(b)(i)



**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



s6(a), 6(b)(i)



*Potential expansion of biometric enrolment*

- NZ currently only captures fingerprints from people in refugee and asylum caseloads, people formally interviewed at the border and people deported from NZ (including criminal deportations). This equates to about 4,000 sets of fingerprints per year enrolled and checked with five country partners.
- Under INZ's proposed Biometric Enrolment Expansion project, there is the potential to increase our annual fingerprint enrolments from the 4,000 to approximately 300,000. INZ is looking at enrolling the fingerprints of people in high identity risk cohorts and of longer-term visa applicants.

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- It is anticipated that the SRTP will eventually be used as a platform to proactively exchange third country national Criminal Deportee data (starting with Convicted Sex Offenders). s6(a), 6(b)(i)

s6(a), 6(b)(i)

- The SRTP could also potentially be used for the sharing of data on goods crossing our borders, without the same privacy constraints.

*Criminal information sharing*

s6(a), 6(b)(i)

- In NZ the Courts own criminal conviction information, and law enforcement agencies have access to this information. While there are restrictions on sharing this information, law enforcement information is shared for intelligence purposes on a case-by-case basis, mainly by Police Liaison Officers based in Five Eyes countries, with verification required through the Mutual Legal Assistance process if it subsequently needs to be used in court. Criminal information is also shared with Australia for vetting purposes, based on the individual's consent.

s6(a), 6(b)(i)

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), 6(b)(i)

**Papers:**

- Data sharing Position Paper
- Annex: s6(a), 6(b)(i)

*Immigration New Zealand, Ministry of Business, Innovation and Employment*

23 July 2019

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## **Agenda item 4: Social Integration, Inclusion and Identity**

**Lead country:** s6(a)

### **Talking points**

- NZ considers breaking down barriers to migrants building networks and connections in their new community, and establishing higher levels of civic engagement, to be the most important elements in achieving successful social cohesion.
- The New Zealand (NZ) Migrant Settlement and Integration Strategy, which was initiated in 2014, is targeted at recent migrants. The intended Inclusion outcome of the Strategy is that “Migrants participate in and have a sense of belonging to their community and to New Zealand”.
- The Inclusion outcome recognises that social inclusion for recent migrants starts with the networks and relationships that are crucial to social interaction. These relationships serve to connect an individual or group with their wider community, helping to facilitate successful settlement and integration and thereby contributing to social cohesion.
- We measure this outcome through a variety of indicators, such as migrants’ sense of belonging, enrolment in clubs and groups, voting participation, and incidences of discrimination. Agencies across the NZ Government provide us with the information, tools and resources to support successful outcomes.
- The NZ Government and other agencies within NZ have established myriad programmes, initiatives, and resources to support the Strategy.

s6(a), s6(b)(i)

## **Background**

- Immigration New Zealand leads the cross-government implementation of the New Zealand Migrant Settlement and Integration Strategy (the Strategy) approved by Cabinet in July 2014. The Strategy is targeted at recent migrants (those in New Zealand for five years or less) and identifies five measurable settlement and integration outcomes: Employment, Education and Training, English Language Proficiency, Inclusion and Health & Wellbeing.
- The Inclusion outcome of the Strategy is that *“Migrants participate in and have a sense of belonging to their community and to New Zealand”*.
- The Inclusion outcome recognises that social inclusion for recent migrants starts with the networks and relationships that are crucial to social interaction. These relationships serve to connect an individual or group with their wider community, helping to facilitate successful settlement and integration and thereby contributing to social cohesion.
- Overcoming the barriers and challenges to migrants building networks and connections in their new community is crucial to the achievement of the Strategy’s Inclusion outcome.
- Civic engagement is also another important element of the Strategy’s Inclusion outcome area. Civic engagement is the ability to participate and contribute to society, both at a community level and broader society level. Civic engagement is about individuals recognising themselves as part of society and taking some responsibility to improve the quality of life for others.
- Agencies across the New Zealand Government provide settlement information, tools and resources to the following to support successful settlement outcomes:
  - New migrants to help them to settle, live and work in New Zealand
  - Employers to help them to prepare for, support and retain their migrant workers
  - Regions to help them plan for, attract and retain migrant workers
  - Communities to help them to create welcoming and inclusive environments for newcomers.

### *Domestic initiatives for social inclusion within New Zealand*

- The Prime Minister and Minister Jenny Salesa (Minister for Ethnic Communities) held an informal meeting with faith leaders on 20 June to seek their input ahead of a series of interfaith dialogues in October/November 2019. The purpose of these dialogues is to discuss how faith leaders and the Government can work together to increase interfaith unity and understanding. At the initial meeting, faith leaders identified some



## RESTRICTED



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

actions they could take together (without the Government), and some issues to discuss further with the Government before agreeing a way forward.

- Evaluation was incorporated as a central component of the two-year pilot of our Welcoming Communities Programme, which supports local government councils and communities to become more welcoming to newcomers. The purpose was to establish a robust evidence base on the effectiveness of the Programme and its contribution to improving social inclusion.
- An independent interim evaluation report, completed in September 2018, provided an assessment of the development, implementation, and early outcomes of the Welcoming Communities pilot. It indicates that Welcoming Communities is on the right trajectory to deliver its anticipated outputs and long term outcomes. Key findings include:
  - local councils taking a more visible leadership role in promoting diversity and inclusion;
  - an explicit shift in the communities from expecting newcomers to 'fit in' to locals taking a 'welcoming' role;
  - a positive change in community perceptions of newcomers and awareness of diversity and inclusion; and
  - growing community engagement and stronger links forming within communities.

### Hate Speech

- In light of the tragic events in Christchurch, you asked officials from the Ministry of Justice to review New Zealand's laws on hate speech. Officials are now actively working on strategies that are intended to further protect those living in New Zealand against acts of terrorism, discrimination, and violence.
- In terms of our current law, the main legislation that covers hate speech in New Zealand is the Human Rights Act 1993. Sections 61 and 131 prohibit the "incitement of disharmony" on the basis of race, ethnicity, colour, or national origin. Other protections against harmful speech are provided by the Harmful Digital Communications Act 2015.
- Justice officials are working with the Human Rights Commission to produce a proposal document. You hope to consult on any options for change early next year. At this stage, no decisions have been made about potential changes to hate speech laws. This is a complex area of policy and we are taking the time needed to get it right. Any changes to the law will need to be carefully considered.

RESTRICTED

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

**Papers:**

- Social Integration, Inclusion and Identity.

*Ministry of Business, Innovation and Employment*

18 July 2019

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## **Agenda item Day 2 (2.5): Industry Roundtable**

**Lead country:** s6(a)

### **Talking points**

- New Zealand is committed to combatting child sexual exploitation and abuse online.
- New Zealand acknowledges that the Digital Industry (in particular mainstream industry/online platforms/providers) are already working to combat child sexual exploitation and abuse (CSEA) online, and this contribution is highly important to our success.
- New Zealand considers good co-design - alongside Digital Industry - is an important factor that will enhance any future digital regulatory regimes. This will assist the operational effectiveness and efficiency with our Digital Industry partners in combating CSEA.
- New Zealand has actively engaged with officials to shape the Industry Roundtable approach so that it focuses on co-design, awareness of current industry engagement, and
- New Zealand agrees with directing the Digital Industry Engagement Senior Officials Group (DIESOG) to undertake further work on the process for implementation of points raised in the Industry Roundtable discussion.

s6(a), s6(b)(i)

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

**Advice**

1. New Zealand acknowledges that Digital Industry (in particular mainstream industry/online platforms/providers) are already working to combat CSEA. The discussions should seek to acknowledge and build on progress to date by industry efforts to combat CSEA.
2. New Zealand, through the Department of Internal Affairs, New Zealand Customs and New Zealand Police work closely together to combat CSEA under a three agency operating protocol. The agencies also work closely with Industry to address this issue wherever possible, nationally and internationally. Nationally, for instance, the Department of Internal Affairs, has an active and collegial relationship<sup>s6(c)</sup> in respect of law enforcement requests for information related to objectionable material, primarily CSEA. Internationally, the New Zealand agencies proactively engage with the Digital Industry on their efforts to remove evidence of CSEA from their platforms and our joint efforts to eliminate ongoing victimisation.
3. To ensure cooperation in combating online CSEA continues and expands, the relationship with Digital Industry requires continued attention, development, and understanding. This is best formed from undertaking a less prescriptive and more collaborative approach to the development of the voluntary principles.

4. s6(a), s6(b)(i)

5.

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

Released under the Official Information Act 1982

---

<sup>1</sup> i.e. Each electronic image has its own unique hash value like a digital fingerprint. A set of hash values can be referred to as a hash set. For Law Enforcement Agencies and Industry this is a means to detect and to block or remove known imagery by its known hash value.

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

**Papers:**

- Position paper: Industry Round Table CSEA Discussion Paper

*Digital Safety Group, Regulatory Services*

*Department of Internal Affairs*

22/07/2019

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

## **Agenda item 6: Countering Foreign Interference – Election Security and Strengthening Democracy**

**Lead country:** s6(a)

### **Talking points**

- Like our Five Eyes partners, New Zealand is focused on the threat of foreign interference, s6(a)
- Our next general election will be held in 2020, and we expect the risk of foreign interference to be higher for this election than for past ones.
- We are interested to understand more about the experiences of our partners in combatting the threats we all face, to help us ensure we can put the necessary protections in place.
- We support continued collaboration amongst our five nations to identify, address and prevent the foreign interference threat.

### **Countering Foreign Interference – Election Security and Strengthening Democracy: key proposals**

s6(a), s6(b)(i)

### **Advice**

*Foreign Interference is a growing risk across all Five Eyes countries.*

1. Foreign interference refers to an act by a foreign state or its proxy that is intended to influence, disrupt or subvert a New Zealand national interest by covert, deceptive or threatening means. In influencing, the objective is to align New Zealand attitudes and

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

policies with the interests of the foreign state. Disruption and subversion, in contrast, may be intended to undermine citizen's trust in democracy and the institutions of state.

2. In New Zealand, concern about the risk of foreign interference has been growing. Free and open societies are vulnerable to interference from states that wish to interfere to advantage their interests or to undermine our values and sow discord. Democracy and the rules-based international order are being challenged by increasingly-confident authoritarian regimes. New Zealand is not immune from these risks.

s6(a)

4. Based on other partner country experiences, there is justification to expect the risk of foreign interference to be higher in the next general election compared to 2017. For example in February 2019 (three months before the Australian federal election), a sophisticated state actor hacked the networks of Australia's three largest political parties.

*The Justice Select Committee is currently reviewing the 2017 election*

5. The Justice Select Committee's routine inquiry into the 2017 General Election has been expanded to consider the risk of foreign interference in New Zealand's democracy. Submissions received have included the framework for political donations (particularly foreign and corporate donations), concerns about email hacking of elected members and political groups, social media activity/regulation/transparency, and general concerns about the vulnerability of New Zealand's democratic institutions to foreign interference.
6. The Select Committee is expected to report later this year. This may inform later stages of preparations for the next general election, or may lead to legislative change, for example in the form of amendments to the Electoral Act 1993. Depending on the timing of the Committee's report there may be a small window to make legislative changes before the next general election.

*Protections for the 2020 election*

7. The Electoral Commission is stepping up its approach to security ahead of the General Election in 2020. The Commission has commenced a programme of work with an expanded focus, including:
  - 7.1. extending its focus beyond preparing for natural disasters and information security to also include security of staff and the public while voting, security of IT infrastructure, and security of physical information (especially live ballot papers)

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- 7.2. extending the notion of security concern to include the integrity of information that the public relies upon in order to freely participate in elections, which is a critical component of the wider resilience of the system against outside interference
  - 7.3. maturing the organisation's security capability, including through working with the Major Events Security Committee (the General Election is considered a major event).
8. The Commission is planning additional steps in 2019 to set in place a solid foundation for security in the 2020 general election:
- 8.1. undertaking a comprehensive Protective Security Threat Assessment, led by an independent security consultant
  - 8.2. setting up a General Election Security Working Group that draws on expertise across government and provides ongoing expertise and support leading up to and during the election. This would include closer collaboration on intelligence issues, including foreign interference risks.
  - 8.3. Running a desktop scenario planning exercise towards the end of 2019. Participants will consider how a response to various security and risk scenarios would be co-ordinated, including roles and responsibilities, decision-making processes, on-the-ground response and channels of communication.
9. s6(a) [REDACTED]
- The Directors-General of NZSIS and GCSB are also providing protective security briefings to all MPs. The briefings focus on improving capability for MPs to identify and protect themselves from foreign interference risks. On risks associated with disinformation, the Electoral Commission will look at providing more information for voters about how to be alert to electoral misinformation and how to check sources. It will also provide more accessible information about where people can complain about content, including online content.
10. In addition, Cabinet has agreed to update the provisions for managing disruptions to elections due to unforeseen or unavoidable events through the Electoral Amendment Bill, to be passed before the 2020 General Election. The current provisions focus on physical disruptions to individual polling places and are no longer fit for purpose. They do not address other disruptive events such as cyber-attacks on the Electoral Commission's infrastructure and systems. The new provisions will:
- 10.1. ensure a more flexible and pragmatic response to a wider range of potential polling disruptions
  - 10.2. maintain the integrity and conduct of electoral processes, and
  - 10.3. ensure those affected by polling disruptions are still able to vote in the election.

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

**Papers:**

- Position paper: Countering Foreign Interference – Election Security and Strengthening Democracy.

*National Security Policy Directorate*

*Department of the Prime Minister and Cabinet*

*15 July 2019*

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

**Agenda item Day 2 (7A): Combating Online Child Sexual Exploitation and Abuse (CSEA)**

**Lead country:** s6(a)

**Talking points**

- New Zealand supports the continued combating of online CSEA.
- New Zealand notes that in our experience, industry (i.e. online platforms/providers) generally engage effectively with the New Zealand Government on this issue. This contribution is important and provides a way to move to the next level collaboratively, s6(a)
- New Zealand—alongside s6(a)—agrees with the interest in expanding cooperation with industry by using the s6(a) approach emphasising co-design. This would allow a focus on technical co-design and the continuation of our current collaborative approach.
- New Zealand supports the proposals s6(a) in regard to combating CSEA and the sharing of technology.
- New Zealand supports the exploration of the financial, technical, and legal implications s6(a)

**RESTRICTED**



**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

**Advice**

**New Zealand's position**

1. New Zealand supports the continued combating of online CSEA.
2. New Zealand is actively engaged in combating the CSEA threat online. This includes the operation of a national filter focused on denying access to foreign websites that host CSEA imagery. New Zealand also undertakes a full range of intelligence, prevention, detection, investigation, and prosecution of persons hosting, creating or sharing of online CSEA content.
3. New Zealand supports the Technology Coalition<sup>1</sup> as a means to share best practice and further cooperation between governments and industry partners.

---

<sup>1</sup> The Technology Coalition was formed in 2006 and is comprised of tech industry leaders (e.g. Facebook, Snapchat, etc) who are represented by individuals who specialise in online child safety issues.

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

4. New Zealand—alongside s6(a) —strongly agrees with the interest in expanding cooperation with industry by using the co-design focused s6(a) approach to the development of voluntary industry principles. This would allow a focus on technical co-design and the continuation of our current collaborative approach.
5. s6(a), s6(b)(i)
- 6.
7. New Zealand supports the exploration of the financial, technical, and legal implications s6(a), s6(b)(i).

**New Zealand's view on improving the combating of CSEA**

8. New Zealand acknowledges that in our experience, industry (i.e. online platforms/providers) tend to engage effectively with the New Zealand Government. However, operational responses (depending on the platform/provider) are not always uniform and effective.
9. This engagement allows New Zealand a largely productive relationship focused on the issue of CSEA. The maintenance of effective relationships requires constant attention and engagement with industry.
10. New Zealand believes that for industry partnership, it is especially helpful that industry partners have the ability to input into co-design of technically focused regulatory regimes.

**New Zealand's position on issues related to CSEA**

***New Zealand's assessment of the online CSEA threat, including grooming and live streaming***

11. For New Zealand, we consider the online CSEA threat to be a significantly high harm and evolving threat. Last year, from the American-based National Center for Missing and Exploited Children (NCMEC) we received just over 3,500 notifications of New Zealand related CSEA content which required further attention or investigation.
12. In regards to other online CSEA threats:
  - For New Zealand, live streaming of CSEA is a difficult form of offending to combat. Perpetrators are predominantly foreign based, often exploiting children they have a relationship with, and there is often no obvious digital footprint that would expose either the parties broadcasting or viewing;

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- Operationally, our focus is on technical solutions but also on industry engagement and engagement with financial institutions that are involved in arranging the payment mechanisms that support these livestream services;
- Legislatively, the issue of live streaming objectionable material (including CSEA) requires attention in New Zealand's media regulatory regime;
- Online grooming is a high harm issue, but from a New Zealand perspective, it is normally acted upon as a criminal matter within our own jurisdiction; and
- Other jurisdictions have stronger legislation related to online grooming (e.g. 'Carly's Law' in Australia that enables prosecution of an adult who lies to a child about their age online).

***New Zealand's approach to effective cross-industry collaboration and technical development***

13. s9(2)(c), 9(2)(g)(i)

New Zealand emphasises the voluntary nature of our interest in collaboration with digital industry.

14. This has been an effective model of engagement in working to combat CSEA to date.

15. We are also having similar success regarding operations to minimise the harm of the Christchurch terrorist attack's digital footprint.

***What are the priority areas for further government data and technology sharing? How should this be funded?***

16. The key priority areas for further government data and technology sharing should include:

• s9(2)(g)(i)

- 
- 
- 
- 
- 

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

**Background**

17. New Zealand is actively involved with operations online to combat the creation and distribution of child abuse imagery and child exploitation material. New Zealand's operations jointly consist of the Department of Internal Affairs, the New Zealand Customs Service, and the New Zealand Police.
18. New Zealand has strong connections to a wide range of international partners (both government and non-government) and is considered a well-respected, effective, and collaborative partner in combatting CSEA.
19. New Zealand runs, through the Department of Internal Affairs, an effective voluntary Digital Child Exploitation Filter that blocks sites for access within New Zealand that host CSEA.
20. In the wake of the Christchurch terrorist attacks, New Zealand has led the Christchurch Call for Action, a commitment by governments and technology companies to eliminate terrorist and violent extremist content online. Initial signatories to the Call include France, New Zealand, Canada, Indonesia, Ireland, Jordan, Norway, Senegal, the United Kingdom, and the European Commission as well as Amazon, Facebook, Dailymotion, Google, Microsoft, Twitter, and YouTube.
21. The success of the Christchurch Call for Action is, in part, based on the willingness of technology companies to engage with governments. <sup>s6(a)</sup>
22. New Zealand is continuing to discuss with industry how best to move forward on the priorities for the Christchurch Call for Action.

**Papers:**

- Position paper: Combatting online child sexual exploitation and abuse.

*Digital Safety Group, Regulatory Services  
Department of Internal Affairs*

11/07/2019

**RESTRICTED**

**Five Country Ministerial 2019  
London, 29-30 July**



## **Agenda item 7B: Preventing and Countering Terrorism and Violent Extremism**

**Lead countries:** s6(a)

### **Talking points**

s6(a)

- On 15 March 2019, New Zealand experienced our largest-ever terrorism attack, allegedly undertaken by a right-wing extremist, espousing anti-Islamist and anti-immigrant views.
- Like our partners, right-wing extremism is a growing problem in New Zealand. We don't have a full understanding of the scale and scope of the problem, and see value in working more closely together as Five Eyes, to better understand the underpinnings of the many and varied ideologies underpinning violent extremism.
- The 15 March terrorist attack was specifically designed to draw in a large social media audience, to draw attention to the causes espoused by the alleged offender. Footage of the incident is still available online, despite ongoing efforts by law enforcement and digital industry.
- We see the Christchurch Call as a catalyst for driving meaningful change in eliminating terrorist and violent extremist content online.
- The Call, where possible, is looking to complement - not duplicate - the excellent work already underway in other fora. We acknowledge all of the countries represented here for their efforts to support New Zealand's work in this area, including the United States who wasn't able to sign up, but who has provided vocal support for the endeavour.

### **Preventing and Countering Terrorism and Violent Extremism: key proposals**

s6(a), s6(b)(i)

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

**Advice**

*The terrorist attacks in New Zealand were allegedly undertaken by a right-wing extremist*

1. The majority of terrorist attacks within the five countries are still undertaken by Islamic extremist groups and their adherents, including Daesh (ISIS) and Al-Qaeda.

s6(a), s6(b)(i)

2. Right-wing extremism however is becoming more common; we are aware that between 2013 and 2017, right-wing extremists were responsible for at least 66 deaths and 113 attacks.
3. In the most recent major terrorist attack within the Five Eyes, on 15 March 2019 in New Zealand, a right-wing extremist allegedly murdered 51 people, injured 50, and will be the first individual charged under the Terrorism Suppression Act.

*We don't share information on right-wing extremism as we do with other security threats*

4. Understanding the threat posed by right-wing extremism is difficult. Numbers on extreme right-wing violence and groups are unclear and probably too conservative. Unlike other terrorist ideologies, the extreme right-wing operates largely as lone actors, doesn't have a set leadership, and individuals hold a broad range of views and ideologies including, but not limited to, racism, anti-Semitism, homophobia, sexism, authoritarianism and anti-democracy

**RESTRICTED**



**RESTRICTED**



5. Different terrorist legal frameworks in each of the Five Eyes means it is difficult to share information about the scale of the threat. For example, in the United States, legal definitions currently only enable “terrorism” action or charges against a person who is a member of a listed Foreign Terrorist Organisation, which excludes domestic actors.
6. The term “right-wing extremist” is complicated for many countries too, with some preferring to describe the phenomenon as white supremacy, ethno-nationalism, or hate groups. A country’s specific political and cultural factors are a further complicating factor, and in all countries, the nature and activities of these groups shades over into legitimate forms of political discourse and activity. It can be difficult to determine the point at which political debate becomes hate speech, and when that in turn becomes terrorism.

7. s6(a)

*The internet is a useful tool for violent extremists*

8. The internet allows for discourse between isolated individuals, and provides anonymity for the expression of polarised views.
9. Internet platforms host significant amounts of extremist content, and their algorithms have been key in providing users with some interest in right-wing extremism with more content. Fringe forums, including 4chan and 8chan, host right-wing extremist discussions which are enabled by a lack of censorship policies. These platforms and forums function as echo-chambers, insulating their users from alternative viewpoints and content.
10. The 15 March terrorist attack was specifically designed to draw in a large social media audience, to draw attention to the causes espoused by the alleged offender. The livestream was designed to go viral and an unprecedented, concerted effort was made by a range of actors to disseminate the video as widely as possible – including through very deliberate efforts to evade detection technologies on social media platforms. Footage of the incident is still available online, despite ongoing efforts by law enforcement and digital industry.

*New Zealand has been driving the ‘Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online’*

11. In response to the online dimensions of the Christchurch attack, the Prime Minister and President Macron launched the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online at a high-level meeting in Paris on 15 May.

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

12. The Call outlines collective, voluntary commitments by governments and online service providers, intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred during and after the Christchurch attack. The Call highlights the need for any action on this issue to be consistent with the principles of a free, open and secure internet and to be taken without compromising human rights and fundamental freedoms. It also acknowledges the important role of civil society in work on these issues.
13. Seventeen countries and the European Commission signed on as supporters of the Call, along with five major US-based tech companies (Microsoft, Twitter, Amazon, Google and Facebook).<sup>s6(a)</sup>
- [REDACTED]
14. We will also look to announce a range of new supporter countries at a side-event in the margins of the United Nations General Assembly, to be hosted by Prime Minister Ardern, President Macron, and King Abdullah II of Jordan.<sup>s6(a)</sup>
- [REDACTED]
15. Following the successful launch on 15 May, our focus is now very much on delivering progress on the Prime Minister's four priority areas ahead of New York in September. The four priority areas are:
- The establishment of a **permanent organisational structure** to take forward the outcomes of the Christchurch Call, potentially building off the Global Internet Forum to Counter Terrorism (GIFCT) but involving governments, tech companies and civil society representatives;
  - The possibility of a new **crisis response protocol** to respond collaboratively and effectively to crises such as the Christchurch attack, with points of contact and agreed procedures to be followed;
  - Gaining a better understanding of existing **research and academic efforts** on terrorist and violent extremist content, and the key areas where more work is needed, potentially empowered by information sharing enabled by increased trust between companies and civil society; and

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

- Exploring what concrete steps might be achieved on **enhancing algorithmic transparency** to better understand possible intervention points to reduce the risk of radicalisation online.

16. The annual GIFCT Conference, held in in San Francisco the week prior to your meeting, will provide an opportunity for the next round of substantive discussions with the tech companies <sup>s6(a)</sup>

s9(2)(g)(i)

17. <sup>s9(2)(g)(i)</sup>

18. <sup>s9(2)(g)(i)</sup>

19. <sup>s6(a), s6(b)(i)</sup>

20. <sup>s9(2)(g)(i)</sup>

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

**Papers:**

- Position paper: Preventing and Countering Terrorism and Violent Extremism.

*National Security Policy Directorate*

*DPMC*

23 July 2019

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## Agenda item: Encryption

Lead country: s6(a)

### Talking points

#### *The 'going dark' problem*


- Strong encryption is a fundamental element of good cyber security, which is increasingly critical to New Zealand's national security and economic prosperity.
- However, strong encryption can impede the access of law enforcement, intelligence, and security agencies to communications critical to conducting their investigations into serious crime, including child exploitation material and terrorist activity.

- s6(a)

s6(a)



s6(a), s6(b)(i)



### **Advice**

1. Strong encryption is fundamental to good cyber security. But it also reduces law enforcement and other agencies' abilities to conduct investigations into serious crime (referred to as 'going dark').

#### *New Zealand's encryption settings*

2. New Zealand's encryption settings are largely in the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). Under s 24 of that Act, there is a duty for New Zealand internet service providers to assist in the execution of interception warrants and other lawful interception. This duty includes decrypting communications where the network operator or service provider has provided the encryption.

3. s6(a)



4.





s9(2)(g)(i)

5.

6.

*Communiqué language*

7. At last year's Five Country Ministerial, Ministers issued a "Statement of Principles on Access to Evidence and Encryption." It has three principles: mutual responsibility (i.e. encryption is a shared issue); rule of law and due process are paramount; and there should be freedom of choice for lawful access solutions.

s6(a), s6(b)(i)

8.

9.

*Shared impact assessment, and assessment of legal and regulatory mechanisms*

10. New Zealand has an established legal position on encryption (as above in "New Zealand's encryption settings"). We are comfortable sharing existing knowledge on legal and regulatory mechanisms.

s6(a), s6(b)(ii)



s6(a), s6(b)(ii)

## Background

15. Encryption, depending on its strength, can make electronic communications data impossible to read or only partially able to be read. Encryption has become more common in everyday use. Strong encryption can also impede access to communications by law enforcement, and intelligence and security agencies. These communications can be critical to conducting investigations into serious crime. Many common online activities (e.g. banking, protection of government information) rely on strong encryption.
16. With increasing demand for secure services, there has been a recent increase in 'end-to-end' or 'client-side' encryption. This is a type of encryption where the provider does not hold its users' encryption 'keys', effectively tying their own hands in terms of being able to access data on their own platform.

### *Increasing use of end-to-end encryption*

s9(2)(g)(i)



*Harmful content, the Christchurch Call, and engagement to date*

19. New Zealand has engaged constructively with online service providers, including social media companies, on harmful content issues following the Christchurch terror attacks, specifically regarding terrorist and violent extremist content online.

s6(a), s6(b)(i)

s6(a), s6(b)(i)

Released under the Official Information Act 1982



s6(a), s6(b)(i)

*CLOUD Act and executive agreements*

29. The United States passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018. The CLOUD Act aims to speed up overseas access to information critical to investigations of serious crime, held by US based global providers. This information could range from terrorism and violent crime to child exploitation material and cybercrime.
30. The CLOUD Act was developed with the support of companies including Microsoft, Apple and Google. It makes explicit in US law the principle that a company subject to a country's jurisdiction can be required to produce its data, regardless of where it is stored. This was an issue in the "Microsoft Ireland" case. Microsoft challenged whether it could be compelled to turn over data stored in a server in Ireland to the FBI.
31. The CLOUD Act authorises the US government to enter into executive agreements with other countries to provide data required for investigations of serious crime. A condition for entering such an agreement is that the US is satisfied the other party has sufficient protections in place for data related to United States citizens. A factor for determining this is whether a country is party to the Budapest Convention on Cybercrime or has domestic laws consistent with the requirements of the Convention.
32. Officials are currently preparing a paper for Ministers seeking Cabinet approval to accede to the Budapest Convention. This is one of the key areas of focus in New Zealand's Cyber Security Strategy 2019. s9(2)(f)(iv), s9(2)(g)(i)



33. s9(2)(j)



34. CLOUD Act agreements are encryption-neutral, neither requiring decryption nor foreclosing governments from ordering decryption to the extent authorized by their laws.

## **Papers**

Attachment 1: Online Safety and Encryption: position paper

*National Cyber Policy Office, National Security Group  
Department of the Prime Minister and Cabinet  
July 2019*

Released under the Official Information Act 1982



## **Agenda item 9: Foreign Terrorist Fighters**

**Lead country:** <sup>s6(a)</sup> [REDACTED]

### **Talking points**

- There are a very small number of New Zealanders who travelled to fight alongside Daesh.
- While there are challenges and uncertainties with the ongoing detention of foreign terrorist fighters and their families in the conflict zone (especially Syria), there are considerable legal and practical hurdles that would make their return and prosecution at home impossible in all but very limited circumstances. The Government would make any decisions concerning New Zealand citizens who has been associated with Daesh on a case-by-case basis.
- New Zealand takes seriously our collective obligations, as reflected in the range of UN Security Council resolutions obliging members to take steps to restrict the movement of foreign terrorist fighters and to ensure they are brought to justice.
- New Zealand is broadly supportive of the battlefield evidence guidelines. They appear consistent with the type of approach NZ takes to obtaining foreign evidence in any mutual assistance case, particularly with regard to protection of human rights.

### **Foreign Terrorist Fighters: key proposals**

s6(a), s6(b)(i)

[REDACTED]



**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

## Advice

s6(a), s6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**

**Five Country Ministerial 2019**  
**London, 29-30 July**



## **Background**

3. There are a very small number of New Zealanders who have travelled to conflict zones to support Daesh and other terrorist organisations. <sup>s6(a)</sup>

4. In respect of New Zealand's obligations under the international counter-terrorism framework, the collective obligation to bring FTFs to justice does not require New Zealand to actively locate, repatriate and prosecute New Zealand FTFs in the current circumstances in Syria.

5. <sup>s6(a), s6(b)(i)</sup>

## **New Zealand policy position on FTFs**

*Cabinet has agreed a policy framework for taking decisions about New Zealand foreign terrorist fighters.*

6. The Cabinet framework has four objectives that should be considered when taking decisions:
- a. Support the protection of New Zealand's national security;
  - b. Bring foreign terrorist fighters to justice, where possible;
  - c. Rehabilitate, where possible; and
  - d. Treat children of foreign terrorist fighters with particular care.
7. Hon Little, as Minister of Justice and Minister Responsible for the NZSIS, is the lead Minister for determining any individual cases.

8. <sup>s6(a)</sup>

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a)

s6(a), s6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**

**RESTRICTED**



**MINISTRY OF BUSINESS,  
INNOVATION & EMPLOYMENT**  
HĪKINA WHAKATUTUKI



**DEPARTMENT OF THE  
PRIME MINISTER AND CABINET**  
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

s6(a), s6(b)(i)

**Children and orphans**

13. Countries are increasingly seeking to remove children from conflict zones, particularly in the cases of orphaned children. s6(a), s6(b)(i)

14. New Zealand may have a small number of children in a similar situation. Officials are currently seeking more information about whether this is the case, and if so, the details of the child(ren). Ministers will be provided with advice, in line with previous Cabinet agreements, before any decisions or actions are undertaken.

**Papers:**

- Position paper: Foreign Terrorist Fighters and Battlefield Evidence

*National Security Policy/International Security Division/Crown Counsel*

*DPMC/MFAT/Crown Law*

11 July 2019

**RESTRICTED**

## FIVE COUNTRY VIRTUAL MINISTERIAL MEETING

**Thursday 18 June 2020, 09:00 – 10:30**

**Pipitea House** s6(a) **Wellington**

## Agenda

To discuss the impact of Covid-19 on key areas of shared concern, including countering hostile state activity, disinformation and Child Sexual Exploitation and Abuse; and to identify further opportunities to collaborate and learn from one another in the immediate and longer term.

[illegible]

~~RESTRICTED~~



	<ul style="list-style-type: none"> <li>Disinformation: how has C-19 changed the landscape or messaging on disinformation? How can we work to ensure public trust is not undermined by disinformation and C-19 is not exploited to further extremist/terrorist agendas of all ideologies, including online?</li> <li>CSEA: Discussion of about the impact of C-19 on the online CSEA threat and next steps following the launch of the voluntary principles.</li> <li>Cybercrime: Discussion on incidents of, and responses to, malicious cyber activity in light of C-19, including cyber fraud, phishing and ransomware.</li> </ul> <p><i>Sequencing</i></p> <p>s6(a)</p> <p>➤</p> <p>➤</p> <p>➤</p> <p>➤</p> <p>➤</p> <p>➤</p> <p>➤</p> <p>➤ <i>Discussion of possible responses and next steps</i></p> <p><b>4.2 Possible for cooperation/deliverables</b></p> <p>s6(a), s6(b)(i)</p> <ul style="list-style-type: none"> <li></li> <li></li> </ul>		<p>5 mins</p> <p>5 mins</p> <p>5 mins</p> <p>5 mins</p> <p>5 mins</p> <p>10 mins</p>
4	<p><b>Encryption</b></p> <p><i>5.1 Update and discussion</i></p> <ul style="list-style-type: none"> <li>Discussion on efforts underway to address the challenges to public safety posed by end-to-end-encryption: update on the proposed international statement.</li> </ul> <p><i>Sequencing</i></p> <p>s6(a)</p>	s6(a)	<p>15 mins</p> <p>3 mins</p> <p>3 mins</p>



	s6(a)		3 mins
	5.2 Possible Areas for cooperation/deliverables		3 mins
	<ul style="list-style-type: none"> <li>Joint approach to international statement on encryption, s6(a), s6(b)(i)</li> </ul>		3 mins
5	<b>Five Country Ministerial</b>  6.1 Update <ul style="list-style-type: none"> <li>Likely timing of next FCM, hosted by New Zealand and discussion on the option to hold additional virtual meetings in the remainder of 2020.</li> <li>Opportunity for Ministers to provide direction on future agenda topics in light of Covid-19.</li> </ul> 6.2 Possible Areas for cooperation <ul style="list-style-type: none"> <li>Joint agreement to begin discussions in ESG and Sherpas on a revised FCM agenda in light of C-19</li> <li>Joint plan to use FCM to follow up on actions and workstreams which occur as a result of this virtual conference</li> </ul> Sequencing <ul style="list-style-type: none"> <li>NZ to provide a brief update on plans for an FCM meeting</li> <li>Other ministers to provide brief comments on future virtual meetings and agenda topics</li> </ul>	NZ	6 mins
6	<b>Next Steps</b> <ul style="list-style-type: none"> <li>Agreed actions and timeframes</li> </ul>	UK	4 mins
			<b>Total:</b> 1h30 hours

**Ministerial Attendees:**

Australia: Hon Peter Dutton, Minister for Home Affairs

Canada: Hon Bill Blair, Minister of Public Safety and Emergency Preparedness  
Hon Marco Mendicino, Minister of Immigration, Refugees and Citizenship

United Kingdom: Rt Hon Priti Patel, Secretary of State for the Home Department

United States: Acting Secretary of Homeland Security, Chad Wolf  
Attorney-General, William Barr





## Agenda Item 1: Welcome and Introductions

*Home Secretary Patel will open the meeting on behalf of the co-chairs, NZ and the UK, and then invite each country to make short remarks.*

### Suggested Talking Points:

- Thank you all for joining us today for this virtual meeting.
- I'd like to first express the sincere condolences of the people and Government of New Zealand to all our Governments and their citizens for the tragic loss of life due to Covid-19, and also to our friends in Canada, following the mass shooting in Nova Scotia in April.
- New Zealand welcomes the close engagement we have had with you on the impact of Covid-19 in recent months, particularly our consular and repatriation response. It is important to work together in the global recovery, based on shared interests in global stability and security, the rules based order and open trade.
- It is a great shame that I will not be welcoming you all to New Zealand for the FCM next month as planned. However, I am pleased that despite all of the restrictions that we face, we are still able to hold these discussions. It may be that this meeting today becomes the new norm of collaborating and coordinating our joint action.
- Covid-19 has had significant impacts for all of us. Impacts on our societies, our health systems and our economies. This meeting is an excellent opportunity for us to learn from one another's experiences over recent months.
- We have put forward an agenda we hope will give us a mutually beneficial understanding of the security impacts of Covid-19 that we are each seeing, in the hope it will lead us to identify closer collaboration and joint approaches to pressing issues of common concern.
- I look forward to our discussions today and to working with you all as we continue to navigate the challenges posed by Covid-19.



## Agenda Item 2: Hostile State Activity during the Covid-19 pandemic

### Discussion

- Perceptions and evidence of the post Covid-19 threat picture, including cyber security threats; and
- Responses to the threat and how we are reacting to changes.

### Possible areas for cooperation/deliverables:

- s6(a), s6(b)(i)
- 

s6(a)

### **Suggested Talking Points:**

- Each of our countries have seen a rise in foreign interference (hostile state activity) in recent years. There has been interference in elections through the spread of disinformation in social media and other platforms to influence public opinion, or more general campaigns to undermine our liberal democracies and free market economies. s6(a)

- s6(a)

RESTRICTED



s6(a)

- So this has been an important area of Five Eyes cooperation. Covid-19 has made it even more important, and I am pleased to kick discussions off with a few points from the New Zealand perspective – both what we are seeing regionally and at home.

s6(a)

- Meanwhile, **businesses that are struggling financially may be more receptive to foreign investment and more vulnerable to foreign acquisition.** Equally, foreign investors may also seek to acquire businesses that are proving successful despite the pandemic, and particularly those that are working on products or technologies valuable in pandemic scenarios.
- To address these concerns, **on our Government brought forward the implementation of two new powers** developed as part of a review of our Overseas Investment Act (a national interest test and ‘call in power’), as well as a temporary new ‘emergency notification regime’ developed to respond to specific Covid-19 related risks. That legislation was passed by Parliament and received Royal Assent at the beginning of June.

RESTRICTED



s6(a)

Released under the Official Information Act 1982

**RESTRICTED**



s6(a)

### Background:

1. New Zealand has taken a range of steps to mitigate risks of interference in our democracy and economy. These include:

- A parliamentary inquiry into foreign interference in our elections. This has recommended a number of changes we are considering;
- Changes to our electoral financing laws to impose further limits of foreign donations, and a commitment to a comprehensive independent review of electoral laws following the 2020 election;

•

s6(a)

•

- The introduction of legislation that will significantly improve Government's ability to manage national security and public order risks arising from foreign investment, including through giving powers to decline any investment already screened if it is contrary to our national interest, and introducing a new temporary notification regime that will allow us to review any controlling investment in a New Zealand business, irrespective of the size of that investment.

### *Foreign Investment in New Zealand*

2. The Covid-19 pandemic is disrupting New Zealand's economy, placing businesses under pressure, and threatening the viability of critical sectors. This increases the opportunity for overseas persons to invest in, or acquire, distressed New Zealand assets in a manner that may not be consistent with New Zealand's national interest (for example, with the purpose of undermining our national security).
3. The Overseas Investment Act 2005 (the Act) manages foreign investment in New Zealand's sensitive assets. The Act traditionally screens investments in sensitive land (such as farm land), significant business assets (those worth at least \$100 million, unless a higher threshold applies under our Free Trade Agreements) and fishing quota.



4. The Government has reviewed the Act with the goal of, among other things, strengthening the Act's ability to manage all foreign investment risks. The Act is unique among Five Eyes partners in offering the Government no ability to manage national security risks, or other risks to New Zealand's national interest.
5. On 12 May the Government announced it would bring forward the implementation of two new powers developed as part of that review to strengthen the Act (a national interest test and 'call in power'), as well as a temporary new 'emergency notification regime' developed to respond to specific Covid-19 related risks. The three powers are summarised in the table below.
6. These changes were enacted in early June and come into effect this month. They will significantly increase our ability to manage efforts by foreign states to disrupt our national security through foreign investment.

Power	Overview
National interest test ( <i>enduring</i> )	<p>A national interest test can be applied to any investment that already requires consent. It will automatically apply to certain high risk investments, such as those with <u>significant foreign state involvement</u>.</p> <p>Transactions found contrary to New Zealand's national interest can have conditions imposed on them, or blocked.</p>
Emergency notification regime ( <i>temporary, for duration of Covid-19</i> )	<p>Overseas persons will need to notify the government of any investment that is not already subject to screening (that is, are worth less than \$100 million), and grants them:</p> <ul style="list-style-type: none"><li>- more than a 25% interest in an existing business;</li><li>- increases an existing holding to 50%, 75% or 100%; or</li><li>- results in the acquisition more than 25 per cent of a business' assets (by value).</li></ul> <p>Transactions found contrary to New Zealand's national interest can have conditions imposed on them, or blocked.</p> <p>Investors should know within 10 days whether their transaction can proceed. If a full national interest assessment is required, this will take an additional 30 days. s6(a)</p> <p>The power will be reviewed every 90 days and remain in place while the Covid-19 pandemic and its associated economic effects continue to have a significant impact in New Zealand</p>
National security and public order call in power ( <i>enduring, once notification regime is removed</i> )	<p>The call in power will allow the government to review certain investments in strategically important businesses (such as critical national infrastructure) that do not require consent under the Act (this differs to the emergency notification regime which will apply to all types of New Zealand business).</p> <p>Unlike the emergency notification power and national interest test, the call in power can only be used to manage significant risks to New Zealand's national security or public order.</p>

s6(a), s6(b)(i)



s6(a), s6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**





s6(a), s6(b)(i)

Released under the Official Information Act 1982

**RESTRICTED**




### Agenda Item 3: Online Harms from Covid-19, including disinformation, Child Sexual Exploitation and Abuse (CSEA) and cyber crime

#### Discussion:

- To discuss how Covid-19 has impacted on a range of online harms and consider joint action to mitigate those harms. Priority issues to cover include:
  - *Disinformation* – how has Covid-19 changed the landscape or messaging on disinformation? How can we work to ensure public trust is not undermined by disinformation and Covid-19 is not exploited to further extremist/terrorist agendas of all ideologies, including online?
  - *CSEA* – Discussion about the impact of Covid-19 on the online CSEA threat and next steps following the launch of the voluntary principles; and
  - *Cyber crime* – Discussion about incidents of, and responses to, malicious cyber activity in light of Covid-19, including cyber fraud, phishing and ransomware.


#### Possible areas for cooperation/deliverables:

s6(a), s6(b)(i)



**Comment:** Each of the Five Countries is experiencing differing levels of online harm resulting from Covid-19. This item will assist in building an understanding of the different impacts we are each experiencing, approaches to addressing these impacts, and opportunities for further collaboration. New Zealand, for example, has not seen significant increases in online harms, and has had good interactions with digital industry to provide safety messages and official communications.

s6(a), s6(b)(i)





### Suggested Talking Points:

#### *Online Harms – what New Zealand is seeing*

- **New Zealand has seen an increase in reporting of low level cybercrime during the Covid-19 pandemic.** CERT NZ, the Government's cyber security one-stop shop, has observed an increased volume of low level cybercrime, with some Covid-19 themed incidents. However, this increase may be due to more reporting, rather than more activity. We have also been impacted by ransomware, including impacts of attacks on Australian companies with New Zealand operations.
- **Online harms, such as CSEA, do not appear to have substantively increased while people have been spending more time online at home.**
- Compared to the same period last year (the seven week period from March to mid-May) **there has been an increase in reporting to Netsafe** on online harms including:
  - a 13% increase in online personal harm (i.e. incidents that cause direct harm to individuals);
  - a 1% increase in community safety issues, (i.e. content that is likely to cause harm to the community e.g. objectionable content);
  - a 32% increase in scams and frauds; and
  - a 42% increase in cyber security issues.

#### *The New Zealand public and Government, have responded*

- There has been **increased public interest in information and tools for staying safe online** since Covid-19. For instance, Netsafe has seen a significant rise in visitors to its site.
- New Zealand's messaging around staying safe online, as a combined effort across government, business and NGOs, has been integrated into the wider pandemic response and communications, and it is hoped that will have a positive effect on online safety.
- New Zealand also has several **significant educational campaigns** are underway to help promote a safe online environment. Many of these developed from concerns that increased time online during lockdown may lead to greater exposure to online harms.
- Two examples of significant domestic campaigns include:
  - a. 'Creating a safe online and digital environment for children and young people,' the Government's public awareness campaign that Facebook supported; and
  - b. 'Stay safe, stay connected' from NetSafe, a New Zealand non-government internet safety organisation, which provides advice on how to avoid scams.
- **CSP's have offered to support to the Government in keeping New Zealanders safe online during Covid19.** For example, Facebook has created a specific 'Covid-19 Information Centre' tab on its app so that New Zealanders can easily access official government information. Google has also promoted Ministry of Health Covid-19 information when users search for related content / advice.



### *Disinformation*

- In general, information related to Covid-19 circulated within New Zealand has been constructive and factual, and from official sources as well as positive media coverage. However, a small number of individuals online continue to attempt to undermine mainstream narratives using false and potentially harmful misinformation related to the Covid-19 pandemic. These users regularly disseminate conspiracy theories regarding the origin, nature, and threat posed by Covid-19 and amplify misleading medical information within New Zealand's information environment.
- **We have seen indications of low levels of deliberate disinformation activity within New Zealand, which has attempted to leverage Covid-19 to promote divisive and inflammatory narratives.** It is highly likely this activity stems from offshore disinformation campaigns, and is not necessarily targeted solely at New Zealand. However, it is also highly likely that individuals or small groups within New Zealand are using Covid-19 as an opportunity to conduct their own smaller-scale disinformation efforts.
- **Covid-19-related online mis and disinformation can have real world consequences,** including inspiring racially-motivated violence, vandalism of telecommunications infrastructure (such as 5G Network Towers, which have occurred in New Zealand and elsewhere) or public acceptance of vaccines (including future Covid-19 vaccines). New Zealand officials are considering how we can be better placed to navigate through these risks in the future, including to safeguard our ongoing public health response, and **we would welcome cooperation with our close partners on information-sharing and considering responses.**
- **We are concerned that Covid-19 has presented an opportunity for extremists to spread misinformation to further their diverse agendas.** The deepening links between Covid-19 disinformation and violent extremism means that the work of the Christchurch Call remains as important, if not more so than it was before Covid-19. New Zealand and France are maintaining our active role in leading this initiative on a multi-stakeholder basis with critical partners in the private sector and civil society.

### *Child Sexual Exploitation and Abuse (CSEA)*

- **New Zealand statistics have shown a slight drop in searches for Child Exploitation Material (CEM).** We are aware that this evidence is different to the pattern seen internationally, with the National Centre for Missing and Exploited Children (NCMEC) reporting an increase in CSEA reports in April 2020. However, more data needs to be gathered to assess whether Covid-19 has impacted rates of CSEA offending in New Zealand.
- **As Five Eyes partners, we need to continue our collective work on ensuring implementation of the 'Voluntary Principles to Counter Online Sexual Exploitation and Abuse'.** This includes further information-sharing, developing tools and solutions, and engaging with technology companies to ensure further adherence to these principles. For example:

s6(a)

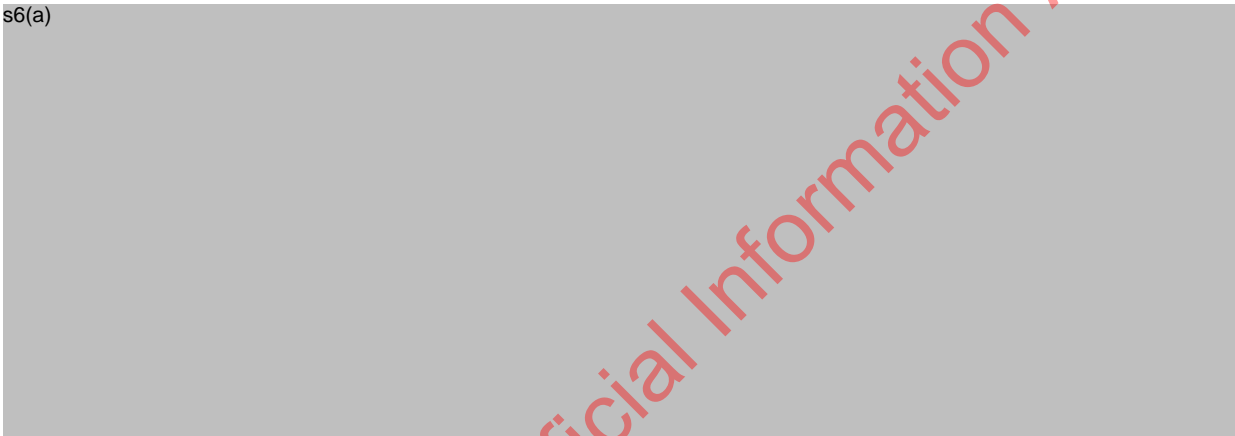


RESTRICTED



- New Zealand will continue to engage with Voluntary Principles signatories to gain insights and track harms to better understand the CEM environment and more effectively target resources; and
- As an ongoing activity in seeking collaborative relationships, New Zealand continues to leverage multi-agency / multi-country groups, such as the Virtual Global Task Force and WeProtect to reinforce messages and support the functioning of our operations.

### Cybercrime

- During the Covid-19 response, **New Zealand agencies have not observed a significant increase in cyber activity targeting or affecting New Zealand organisations and are not aware of any imminent threats.** However, there has been an increased in reporting of low level cybercrime to CERT NZ.
- s6(a)  

- CERT NZ and Consumer Protection are jointly developing an awareness initiative, which will include TV broadcasting material, focussed on building the cyber security capability and confidence of businesses and consumers.
- The exploitation of this crisis by malicious actors reinforces the need for strong international cooperation on cybercrime, particularly where this takes place across borders. New Zealand is continuing work on accession to the Budapest Convention on Cybercrime and we hope to be in a position to make a statement on this soon.

### Background:

#### Online harms

1. The additional time New Zealanders are spending online during lockdown increases their risk of exposure to online harms (e.g. scams). These harms also include children and young people accessing inappropriate content like pornography and exposure to malicious activities such as child grooming.
2. N4L reported an increase in the number of blocks per student during lockdown for every threat category – phishing, command and control, malware, anonymizers and DNS exfiltration.  
*[Phishing relates to sites that aim to trick users into giving out sensitive information such as usernames and passwords. Command and control (C&C) is where the user's device is being controlled by a bad actor / botnet. Malware is a broad category of software that is designed to cause harm to the device or permit the device to be taken over for other purposes.]*

RESTRICTED





*Anonymizers permit the user to act anonymously, thus bypassing filtering and other safety or monitoring mechanisms. DNS exfiltration is where potentially sensitive data is funnelled through DNS queries, trying to bypass security measures to get it through to a third party.]*

3. There are several internet safety campaigns underway, some of which were developed by the Government in response to concerns that Covid-19 would increase New Zealanders' exposure to online harms.
4. One of these Government-developed campaigns is 'Creating a safe online and digital environment for children and young people,' which aims to support parents and carers to protect their children from online threats, including bullying, grooming and access to inappropriate material.
5. This campaign was launched in June, and will continue to be rolled out in two phases:
  - a. Phase 1 – targeted messages for parents and caregivers, providing information and tips to support them in creating a safe online environment for whanau, specifically children and young people (June – July 2020); and
  - b. Phase 2 – targeted messages directed at children and young people to support them in identifying, managing and, where appropriate, reporting online risks and harms (to run over 12 months).
6. This is a multi-channel campaign using TV, TV on-demand, print ads in newspapers, social media, YouTube, radio, billboards, posters and Google search engine optimisation. s9(2)(ba)(i)  
[REDACTED]  
[REDACTED]
7. Netsafe launched the 'Stay Connected, Stay Safe' education campaign in the first week of lockdown to provides tips and advice on how to safely use the internet to stay engaged.
8. The Office of Film and Literature Classification (OFLC) has also created online resources to support parents and carers in restricting children's access to inappropriate content and educating their children on the negative side of watching pornography.
9. CSPs have supported Government in providing public safety during Covid-19. Facebook created a specific 'Covid-19 information Centre' tab on its app so that New Zealanders can easily access official Government information.
10. Facebook has also recently extended some of its services to New Zealand, including its third-party checking programme and its messaging app for children. While the extension of these programmes was arranged prior to Covid-19, they are particularly useful during the Covid-19 environment. The third-party checking programme can be useful in countering Covid-19 related misinformation and a messaging app for children is particularly important while children are spending more time online during lockdown.
11. Microsoft created an international online safety campaign in collaboration with international companies and endorsed by the Five Countries Ministerial officials group. The international campaign, 'Stay safe at home. Stay safe online,' went live on the 18 April 2020 and aims to help keep children and young people safe from online exploitation during Covid-19.
12. Google has helped to ensure New Zealanders are provided with accurate and timely information related to Covid-19 through its search result system and app verification process. Google has been working with Government to ensure public health messages appear right across Google – through organic search results, SoS alerts and ads. For example, on the 25th of March Google featured a link directly to the Government's Covid-19 website and on the 26th and 27th of March Google had the text 'Stay home and help stop coronavirus' on its

RESTRICTED



homepage. Additionally, Google has prioritised the review and publication of New Zealand Government apps relating to Covid-19.

#### *Disinformation*

13. Right-wing extremists have used the crisis to spread hate and conspiracies. Internationally this has included anti-Chinese racism, theories that the virus was deliberately started or spread by traditional enemies such as Jewish people or the “Deep State”, and claims that the pandemic is less serious than stated and governments are using it to enforce authoritarian measures.
14. The crisis is also being used to enforce extremist narratives such as “accelerationism” (the idea that democracy is a failure and mobilising social conflict can speed up its end), and the need for change in the world order.

#### *Child Sexual Exploitation and Abuse (CSEA)*

15. We need to continue and expand information-sharing on key trends observed in CSEA and law enforcement methods. There is also opportunity to work more collaboratively to improve and invest in innovative tools and solutions to respond to the evolving threat and changing societal and offending behaviours.
16. We also need to collectively focus on progressing uptake of the CSEA voluntary principles by digital industry (for example, targeting the livestreaming of CEM) by collaborating with and holding technology companies to account for their commitments.
17. The Department of Internal Affairs (DIA) leads New Zealand’s engagement with the Five Eyes on this. DIA currently has a positive close working relationship with s9(2)(j) in relation to addressing child exploitation matters, and has engaged with s9(2)(j) on legislative proposals to counter violent extremist content online. s9(2)(j) provided constructive feedback in the development of proposals to the Films, Videos and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill, which, if enacted, will provide additional regulatory and enforcement tools to remove harmful content that is livestreamed or hosted by online content hosts.

#### *Cyber Crime*

18. Overall levels of malicious cyber activity remain relatively constant. Some Covid-19 specific lures and themes have emerged, though agencies have not seen large volumes of Covid-themed malicious activity. However, this situation could change at any time and New Zealand is not immune from opportunistic malicious activity or targeted attacks.
19. The NCSC is monitoring Covid-19 related cyber security guidance from a range of international sources and passing it on to public and private sector customers either directly or via notifications and news updates on the NCSC website. CERT NZ and the NCSC have published warnings on their websites about Covid-related malicious activity, and are updating guidance on good cyber hygiene practices regularly, particularly for those who are working remotely.

20. s6(a)



21. It is likely that in many respects, online habits will not revert to what they were pre-Covid-19, because social engagement and the economy have changed so significantly. Building

RESTRICTED





capability and confidence in operating securely online in a time of accelerated digital technology use is a prerequisite for increasing the productivity of businesses operating digitally. CERT NZ and Consumer Protection are jointly developing an awareness initiative, which will include TV broadcasting material, focussed on building the cyber security capability and confidence of businesses and consumers.

22. New Zealand has expressed an interest in acceding to the Budapest Convention. Accession would enhance our access to information for criminal investigations, as well as information on best practice for cybercrime investigations and threat trends. Cabinet will make a final decision on accession after a consultation period.

23

s9(2)(f)(iv)



*Implications of Covid-19 for Countering Violent Extremism (CVE)*

24. Those spending more time online in self-isolation risk increased exposure to extremist content and radicalisation, particularly people rely on the internet for news, updates and social contact. This is of significant concern as extremists online have encouraged attacks against target communities, including deliberately spreading the virus.
25. There are also likely to be significant short-term and enduring mental health implications arising from the pandemic and restrictions such as lockdowns, potentially making those individuals with extremist views more vulnerable to radicalisation.
26. Islamic extremists have also sought to use the pandemic for their own purposes. Initially, Da'esh / ISIL warned its supporters to stay away from Europe, to avoid becoming infected and therefore preserving ISIL forces for future attacks. However, more recently ISIL has encouraged supporters to take advantage of the pandemic by launching attacks where there are fewer security measures.
27. For New Zealand, these developments highlight the importance of implementing several existing work streams to deliver our national CT/CVE Strategy:
- a. Social inclusion (led by MSD). Promoting an inclusive society through government and non-government initiatives will build the resilience required to counter emerging extremist narratives. Promotion of public messages such as "Be kind".
  - b. CVE online (DIA). The potential exposure of increased numbers of New Zealanders to extremist material online requires prioritisation and the utilising greater technology and digital methods where possible.
  - c. Christchurch Call (MFAT, DPMC). New Zealand and France are maintaining our active role in leading the Christchurch Call on a multi-stakeholder basis with critical partners in the private sector and civil society.
  - d. Disengagement (NZ Police) and broader CVE frameworks (DPMC). Our reduction framework needs to adapt to potentially higher numbers of individuals with extremist views.



- e. Crowded Places Strategy (NZ Police). The on-hold launch of the Crowded Places Strategy, adapted to reflect changes such as the heightened risk to supermarkets and hospitals, should be prioritised once alert level restrictions allow.
- f. Safer Communities Fund (DIA) and community engagement. s6(a)

[Redacted text block]

Released under the Official Information Act 1982



## Agenda Item 4: Encryption

### Discussion

- Discussion on efforts underway to address the challenges to public safety posed by end-to-end encryption: update on the proposed international statement.

### Possible areas for cooperation/deliverable:

- Joint approach to international statement on encryption, s6(a), s6(b)(i)

s6(a), s6(b)(i)

### **Suggested Talking Points:**

#### *Encryption*

- New Zealand shares the concerns of the Five Countries and other likeminded nations about the impact of end-to-end encryption on our ability to protect citizens from harm. We also recognise the need for strong encryption, which enables commerce, improves cyber security, and protects the privacy of our citizens' and government data.
- We welcome the most recent updates to the text of the draft statement on encryption and public safety, and the willingness of s6(a) to keep negotiation of the text open to ensure broad support from likeminded countries.
- s6(a), s6(b)(i)
- 
- New Zealand continues to work on addressing the public harm associated with encrypted communications. Officials are engaging with other likeminded partners to understand their approach, s6(a), s6(b)(i)

RESTRICTED



s9(2)(f)(iv)

**Background:**

1. Encryption policy seeks to balance protecting the privacy and security of citizens and business while addressing the ability of malicious actors, including those involved in child exploitation, to act in secret.
2. The Five Countries have made a number of collective statements on end-to-end encryption, however, there has not been a substantive change in position by the technology industry, including s9(2)(g)(i), on mitigating the public safety issues arising from increasing encrypted messaging.

*New Zealand has been asked to sign a joint statement on encryption*

3. s6(a) has drafted a statement urging technology companies, including Facebook, to embed public safety in system designs, to allow companies to act against illegal content on their platforms, and to enable law enforcement access to content. The statement asks companies to stop implementation of end-to-end encryption until they can ensure their design meets the objectives above.
4. The statement is a follow up to the open letter to Facebook on end-to-end encryption, signed by the UK, United States and Australia in December 2019, and earlier statements from the Five Country Ministerial meetings in 2018 and 2019. s6(a)

5. s9(2)(g)(i)

6. s6(a)


*The statement is still under negotiation* s6(a)

7. s6(a)

8. s6(a), s6(b)(i)



9. s6(a), s6(b)(i)



*New Zealand's next steps on the issue of encryption*

10. As well as ongoing engagement with Five Eyes partners, officials are undertaking the following ongoing engagement:

s6(a)



11. New Zealand officials are also developing a policy work programme to fully scope the current issue faced by agencies as end-to-end encryption becomes ubiquitous (leading to more investigative data becoming unavailable), and investigate potential solutions that also protect security and privacy.



## Agenda Item 5: Five Country Ministerial

### Update

- Likely timing of next FCM hosted by New Zealand, and discussion on the option to hold additional virtual meetings in the remainder of 2020; and
- Opportunity for Ministers to provide direction on future agenda topics, in light of Covid-19.

### Areas for cooperation

- Joint agreement to begin discussions in ESG and Sherpas on a revised FCM agenda in light of Covid-19; and
- Joint plan to use FCM to follow up on actions and workstreams which occur as a result of this virtual conference.

**Comment:** *This item provides you the opportunity to reiterate New Zealand's commitment to hosting the Five Country Ministerial and Quintet of Attorneys-General, when circumstances allow a face-to-face meeting. It is also an opportunity to test Ministers views on further virtual meetings, and invite Ministers to discuss, in light of Covid-19, the priorities they wish to see progressed through future calls and the Five Country Ministerial.*

s6(a)

### **Suggested Talking Points:**

#### *New Zealand's hosting of FCM 2020*

- As I said in my opening statement, it is a great shame that my ministerial colleagues and I are unlikely to be able to host you all in New Zealand, later this year.
- New Zealand officials will continue to work with partners to identify an agreeable path to holding an in-person FCM in New Zealand, as soon as it practicable.
- The most likely option, to give sufficient time for border measures to be relaxed and international travel to be resumed, is July 2021, which would be a return to the usual hosting cycle.
- In the meantime, I think this virtual meeting has been extremely useful, and as current FCM Chair I would welcome the opportunity to host another such meeting this year, as our calendars allow.
- I suggest we identify a small number of priority issues we would like to address collectively at a future call, ahead of an in-person meeting.
- One of the first topics we chose could be a more detailed discussion on the border and migration issues arising from Covid-19.

**When discussion has concluded, invite the facilitator s9(2)(a) to summarise agreed action points and next steps.**

RESTRICTED



## Agenda Item 6: Next Steps

**The UK Home Secretary will close the meeting.**

s6(a)

### Suggested Talking Points:

- I would like to thank you all for making yourselves available for this meeting, and for your contributions to make these discussions so insightful and beneficial to us all.
- Together we have gained true insights into each other's experiences in countering the Covid-19 virus, and I believe we have identified shared concerns and put forward new, joint actions to address these ever-evolving threats to our national security.
- I support further engagement at the Ministerial level, as and when diaries allow. The New Zealand Parliament will rise and be dissolved in early August, ahead of our General Election in September, which is followed by the American Presidential Election in November.
- I hope that we can meet again at a mutually agreeable time to discuss different topics of mutual concern.
- Finally, particular thanks to my Co-Chair, Rt Hon Priti Patel, for proposing this virtual meeting take place.

*Department of the Prime Minister and Cabinet,  
NZIC, Department of Internal Affairs,  
Ministry of Foreign Affairs and Trade, The Treasury*

*June 2020*

RESTRICTED





**ATTACHMENT A**

**Virtual Five Country Ministerial Meeting – Draft Communique**

s6(a)

Released under the Official Information Act 1982

**RESTRICTED**



s6(a)

Released under the Official Information Act 1982



## ATTACHMENT B

### New Zealand's approach to Covid-19

*Comment: Due to the reduction in time available for this meeting, an agenda item on Covid-19 updates from each country has been removed. Despite this, you and your colleagues may still wish to discuss this, as the stage each country is at with their Covid-19 response will impact both how the Five Countries are able to work together, and the national security impacts experienced.*

*This attachment provides suggested talking point and background information to draw from, if this does come up.*

#### Potential Talking Points:

##### *New Zealand's response to Covid-19 and strategy to emerge from lockdown*

- Although New Zealand has benefitted from our geographical location and not having the virus on our shores until later than others, our deliberate, **"go hard, go early" strategy** saw New Zealanders work hard to combat Covid-19, and as a result, **we now have no active cases of Covid-19 in New Zealand.**
- We remain vigilant, prepared to respond to a further outbreak or evidence of community transmission, if they occur. We have a **four-level Alert Level system** which frames our response and will allow us to move quickly again if we need to.
- To achieve elimination, New Zealand implemented a **full lockdown**. This involved shutting the borders to all but returning New Zealanders, and enforcing a maximum containment policy where the entire population, other than essential workers, were required to stay at home except for medical reasons, food supplies and daily exercise. People were unable to visit family and friends, even in cases of serious illness and death. This full lockdown lasted four weeks.
- We then spent two weeks at Level 3, with some partially relaxed restrictions. Under Alert Level 2, which we spent three and a half weeks at, restaurants, beauty providers, schools and education providers were able to open.
- We removed to Alert Level 1 on 8 June, with virtually all restrictions lifted. The focus under Alert Level 1 is on:
  - Robust border controls
  - Continued surveillance and testing
  - Contact tracing and rapid isolation of any new cases
  - Public support to prevent any further spread, including good hygiene and keeping records of movement.
- New Zealand's **economy is open**. All limits on our normal freedoms to combat Covid-19 (such as social distancing and gathering restrictions) are lifted. Our economy is recovering, and our borders remain open for the trade of goods. Even so, our economy will take a significant hit, from both the lockdown and the impact of the virus itself. We have allocated \$62.1 billion (across an initial package and Budget 2020 measures) to support New Zealanders through this crisis. Our focus is on supporting individuals and businesses, strengthening the health system, helping industries and sectors that have lost their funding

base due to Covid-19, and ensuring core services and infrastructure are funded to meet New Zealanders' needs.

#### Border measures

- As part of our “go hard, go early” strategy, New Zealand closed its borders to foreign nationals on 19 March. We did this to save lives and prevent the worst social and economic outcomes. This included returning New Zealanders going into a 14-day period of self-isolation or quarantine. We further implemented a requirement for Government managed isolation or quarantine from 10 April. However, although these restrictions were successful in their aim, they have also had significant economic and social consequences for the country.
- An open border currently presents significant risks to public health. However, international connectivity is fundamental to New Zealand's economic and social well-being, and we need to reconnect with the world by lifting border measures when it is safe to do so. Public health considerations will continue to be prioritised.
- No decisions have yet been taken on reopening our border. Our Government has developed a set of **flexible guiding principles** to manage border settings in the longer term, calibrated to existing public health conditions. These include:
  - protecting New Zealanders from Covid-19 and minimising the risk that Covid-19 is re-introduced through the border;
  - mitigating the risk of Covid-19 transmission to the Pacific;
  - ensuring goods move into and out of New Zealand at all Alert Levels to maintain connections to key trade markets; and
  - facilitating increased people movement in and out of New Zealand, as public health considerations allow.
- We are also working through an exemptions framework for workers with skills that are essential to economic recovery and scenarios for isolation and quarantine for those entering our country.
- In line with this principles-based approach, **New Zealand aims gradually to re-establish connections with countries that are Covid-19 free or where the virus has been contained or eliminated.** We are keen to hear from others on how they are looking to re-establish global connectivity.

#### Background:

Overview: Covid-19 in each country

Country	Cases <sup>2</sup>	Deaths	Projected GDP growth (annual, from April 2020) <sup>3</sup>
Australia	7,285	102	-6.7%
Canada	98,720	8,038	-6.2%
New Zealand	1,504	22	-7.2%
United Kingdom	291,588	41,213	-6.5%
United States	1,999,900	112,895	-5.9%

<sup>2</sup> Source: John Hopkins University. Correct as at 11 June 2020.

<sup>3</sup> Source: International Monetary Fund, World Economic Outlook (April 2020)



*New Zealand's elimination strategy*

1. New Zealand has a national policy of eliminating Covid-19 from the country. From an epidemiological perspective, 'elimination' means there are zero new cases in a location.
2. New Zealand benefitted from being able to see the virus move in Asia and Europe for some weeks before it hit our shores, with our first recorded case being a passenger arriving from the Middle East on 28 February.
3. That additional time, and our geographic isolation, assisted with our elimination of the virus, but the decision to lockdown borders and quarantine everyone in their homes was crucial – and a decision not taken lightly. The powers required to implement this lockdown, Level 4 in particular, are some of the most powerful that a state can exert over its people, and limit freedoms guaranteed in the Bill of Rights Act 1990.
4. The decision to pursue an elimination strategy was announced on 23 March. On 25 March an Epidemic Notice was issued and a State of National Emergency was declared, giving significant powers. Constraints on people were detailed. To achieve elimination, New Zealand moved to Alert Level 4 (full lockdown) for one month, before spending another two weeks at Alert Level 3.
5. The elimination strategy relied on community-based compliance, rather than enforcement from Police, i.e. widespread buy-in that this is the right thing for everyone to do, including to monitor and self-enforce. This was backed up with extensive Government communications and clear guidance, simple and clear expectations, and significant supporting information.
6. The Prime Minister and Director-General of Health fronted a media stand-up almost every day of the week, to provide consistent and trusted advice on the state of the virus, including the number of new cases and any deaths, and to answer media questions.
7. In addition, New Zealand ran one of the largest media campaigns the country has ever seen, with television, print and radio advertising, billboards, and a dedicated website. The communications campaign was crucial to achieving compliance with the restrictions, and in turn, eliminating the virus.
8. Significant efforts were made to test people for Covid-19, to ensure there isn't undetected community transmission. Accordingly, New Zealand had one of the highest testing rates per capita of any country in the world, at 48.5 per thousand people, which is ahead of all other Five Country partners.
9. Cabinet set a clear framework for moving down – or back up – alert levels, based on eight criteria: trends in the transmission of the virus;
  - the capacity and capability of our testing and contact tracing systems;
  - the effectiveness of our self-isolation, quarantine and border measures;
  - the capacity in the health system more generally to move to the new level;
  - evidence of the effects of the measures on the economy and society more broadly;
  - evidence of the impacts of the measures for at risk populations in particular;
  - public attitudes towards the measures and the extent to which people and businesses abide by them; and
  - our ability to operationalise the restrictions.



10. We relied on a mix of existing and new legislation to enforce the lockdown and subsequent alert levels. New legislation and subordinate instruments were enacted throughout the lockdown, both to manage the Covid-19 situation, but also the consequences of the lockdown. A special Parliamentary select committee was established to scrutinise Government action while Parliament was able to sit.

*Keeping the economy functioning*

11. The impact of the lockdown was such that a banking crisis was feasible, and a majority of New Zealand businesses were under significant stress.
12. The Government announced a range of support measures for businesses, including a wage subsidy scheme available to all business with a 30 percent drop in revenue attributable to the Covid-19 outbreak, if they made best endeavours to pay at least 80 percent of each employee's normal wages or salary.
13. The \$12.1 billion package of support announced on 17 March included:
- Initial \$500 million boost for health services
  - \$5.1 billion in wage subsidies for affected businesses in all sectors and regions
  - \$126 million in Covid-19 leave and self-isolation support
  - \$2.8 billion income support package for our most vulnerable, including a permanent \$25 per week benefit increase and a doubling of the Winter Energy Payment for 2020
  - \$100 million redeployment package
  - \$2.8 billion in business tax changes to free up cash flow, including a provisional tax threshold lift, the reinstatement of building depreciation and writing off interest on the late payment of tax; and
  - \$600 million initial aviation support package.
14. The \$50 billion Covid-19 Response and Recovery Fund, as part of Budget 2020, builds on the \$12.1 billion package, to progress further measures, including:
- \$6.9 billion to extend the Wage Subsidy Scheme
  - A Business Tax Relief Package of \$1.9 billion
  - \$186 million across the education sector, and
  - A number of other packages to support the short-term response of the health, aviation and social sectors.

*Impacts of the border closure*

15. Closing New Zealand's borders to most people movement bought us time to stop the importation of the virus, slow its spread, and eliminate it from New Zealand. International passenger arrivals dropped from around 20,000 people per day to fewer than 200 people, and on occasion, no entries. People arriving have entered managed isolation or quarantine.
16. The border closure severely impacted industries reliant on international people movement: in particular, aviation, tourism and international education. New Zealand's social fabric has also been affected, as many citizens have close family and friends overseas.

*Reopening of our borders*

17. Our success in pursuing elimination of Covid-19 means we are in the enviable position of being able to 'reopen' the domestic economy, but our borders will remain closed for some time.



Under Alert Levels 2, 3, and 4, and now Level 1, New Zealand's international borders remain closed to foreign nationals, with few exceptions – but open to goods and New Zealanders returning home.

18. No final decisions have been made about the reopening of borders. We expect that it will take many months for our borders to reopen in a significant way to people movement, and extensive quarantine requirements may be imposed. The timing of a reopening will depend on the status of Covid-19 in other countries, and the development of a test, vaccine or cure.
19. Prime Ministers Ardern and Morrison have committed to opening a Trans-Tasman safe travel zone, once both countries are in a position to do so. Such an arrangement would be put in place once it is safe to do so and necessary health, transport and other protocols had been developed and met, to ensure the protection of public health. Policy work has commenced in both countries to develop details for how this will work in practice.
20. This may also be able to be extended to a "Pacific bubble". New Zealand has received approaches from other countries interested in establishing connections to facilitate the movement of people and goods (for example, Fiji). Our response to such approaches will be country-neutral, based on our guiding principles.

#### *Engagement with partners*

21. Across the All-of-Government Covid-19 response there has been engagement with Five Eyes partners, particularly in the Five Nations consular space but also in sharing experiences of our respective domestic responses and on the international recovery from Covid-19.
22. There has been extensive engagement and coordination with Australia, as illustrated by the PM Ardern's participation in a meeting of the Australian National Cabinet (the first time since WWII) in working towards a Covid-safe Travel Zone. We also have close and regular engagement with UK, US and Canadian colleagues at all levels on our respective domestic responses and the international recovery, including on international cooperation on vaccine development.
23. These partnerships will be crucial to New Zealand in our recovery, given the need to work with like-minded partners on upholding the rules based order and promoting open trade.





## ATTACHMENT C

### Latest draft of international statement: end-to-end encryption and public safety

s6(a)

Released under the Official Information Act 1982

RESTRICTED

Released under the Official Information Act 1982